Ajuntament de Barcelona

Acció Social

GUIA DE BONES PRÀCTIQUES – TRACTAMENT DE DADES DE CARÀCTER PERSONAL

ÍNDEX

1. Introducció

1.1. L'entitat i la LOPD

La Direcció de Serveis d'Acció Social (en endavant, Acció Social), organisme dependent de l'Àrea d'Acció Social i Ciutadania, de l'Ajuntament de Barcelona, amb seu a l'Avinguda Diagonal, 233, consta de quatre departaments (Serveis Socials Bàsics, Atenció a Persones Vulnerables, Atenció a la Gent Gran i Atenció a l'Infància, Adolescència i Famílies) i un servei (Urgències i Emergències).

Acció Social posa en marxa un conjunt de polítiques orientades al benestar de les persones, estructurades a partir del Pla municipal per a la inclusió social i un conjunt de programes que, segons les temàtiques més concretes o els col□lectius de població, van desplegant els objectius i les actuacions que doten de contingut l'acció social de l'Ajuntament

L'aplicació de la LOPD en el sector dels Serveis Socials té diverses particularitats:

- Les dades de caràcter personal tractades són de nivell alt.
- És habitual que les dades es cedeixin o comuniquin de forma legítima a altres Administracions Públiques.
- Els fluxos de dades en paper són habituals, fet que dificulta la custodia.
- Existeix una elevada deslocalització geogràfica de la xarxa de centres socials.
- És habitual que la tramitació administrativa la realitzin terceres persones en nom dels afectats o beneficiaris dels serveis.
- Existeixen nombrosos serveis concertats o externalitzats en el sector privat i ONGs.

1.2 Contingut del document

En aquest document es pot trobar el següent material:

- Una "Guia de Bones Pràctiques i de Formació General als Professionals" destinada a tots els professionals que en el seu treball habitual tracten dades de caràcter personal.
- Una "Guia de Bones Pràctiques i de Formació General als Responsables" destinada als caps i responsables de departaments, àrees o serveis, i al personal amb responsabilitat en el tractament de dades de caràcter personal.
- Una "Guia de desenvolupament d'aplicacions" que tractin dades de nivell alt.
- Un "Decàleg de Bones Pràctiques en Protecció de Dades de Caràcter Personal" destinat a totes les persones, tractin o no dades de caràcter personal.
- Les clàusules estàndard de protecció de dades de caràcter personal a incloure en tots els procediments de recollida de dades a Acció Social i en tots els contractes de prestació de serveis.
- Procediment de declaració de creació/modificació/baixa de fitxers de dades de caràcter personal.

2. Guia de Bones Pràctiques i de Formació General als Professionals

Aquest capítol va adreçat a tots els professionals que en el seu treball habitual tracten dades de caràcter personal.

L'objectiu d'aquesta guia és oferir una idea general de la Llei Orgànica de Protecció de Dades (LOPD), els seus principis bàsics, les mesures de seguretat que cal aplicar sobre les dades de caràcter personal (DCP) i com actuar en la operativa diària per tal de complir els requeriments de la normativa vigent en matèria de protecció de dades.

2.1. Introducció a la Protecció de dades

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (des d'ara LOPD) té per objecte, garantir i protegir, en el que concerneix al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i intimitat personal i familiar.

La protecció de les dades personals és un dret fonamental que afecta a qualsevol tipus de dada, sigui íntima o no, i com a tal és irrenunciable i preval sobre qualsevol altre dret.

L'aplicació de la LOPD en el sector dels Serveis Socials té diverses particularitats:

- Les dades de caràcter personal tractades són molt sensibles.
- És habitual que les dades es cedeixin o comuniquin de forma legítima a altres Administracions Públiques.
- Els fluxos de dades en paper són habituals, fet que en dificulta el control i la custodia.
- Existeix una elevada deslocalització geogràfica de la xarxa de centres socials.
- És habitual que la tramitació administrativa la realitzin terceres persones en nom dels afectats o beneficiaris dels serveis.
- Existeixen nombrosos serveis concertats o externalitzats.

2.1.1. Normativa aplicable

A fi de garantir la necessària seguretat jurídica en un àmbit tan sensible per als drets fonamentals dels ciutadans com és el de la protecció de dades, existeix un legislació complexa d'obligat compliment tant per al sector públic com privat entre la qual destaquen:

- Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.
- Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

2.1.2. Definicions

Dades de caràcter personal: Qualsevol informació concernent a persones físiques identificades o identificables.

Tractament de dades: qualsevol operació o procediment de caràcter automatitzat o no que s'apliqui a dades personals.

Fitxer de dades personals: qualsevol conjunt estructurat de dades personals, independentment de la seva modalitat de creació, emmagatzemament, organització i accés.

Comunicació o cessió: tota revelació de dades personals feta a una persona diferent de l'interessat.

Afectat o interessat: persona física titular de les dades que siguin objecte de tractament.

Responsable del fitxer: persona física o jurídica, pública o privada, o òrgan administratiu o unitat funcional que decideixi sobre la finalitat, contingut, ús i tractament de dades personals.

Encarregat del tractament: aquella persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, individualment o conjuntament amb d'altres, tracti dades personals per compte del responsable del fitxer.

Usuari: qualsevol persona física o procés autoritzat a accedir a dades o recursos.

2.1.3. Àmbit d'aplicació

Dades de caràcter personal registrades en suport físic, que les faci susceptibles de tractament, i tota modalitat d'ús posterior d'aquestes dades pels sectors públic i privat.

No aplica a:

- Fitxers mantinguts per persones físiques en l'àmbit exclusivament personal o domèstic.
- Fitxers sotmesos a la normativa sobre protecció de matèries classificades.
- Fitxers establerts per a investigacions del terrorisme i delinqüència organitzada.

2.2. Principis de protecció de dades

2.2.1. Qualitat de les dades

Les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut.

Per tant:

- Cal definir inicialment la finalitat per a la qual es vol recollir les dades.
- No es poden utilitzar les dades per a una finalitat diferent a aquesta.
- No s'han de recollir dades que no siguin necessàries per a aquesta finalitat.
- Les dades han de ser exactes i veraces, en cas contrari s'han de cancel□lar i substituir d'ofici.

Les dades personals han de ser cancel□lades un cop deixin de ser necessàries o pertinents per la finalitat per la qual havien estat recollides. No obstant, es podran conservar durant el temps en què es pugui exigir algun tipus de responsabilitat derivada de:

- Una relació o obligació jurídica,
- l'execució d'un contracte, o bé
- l'aplicació de mesures pre-contractuals sol□licitades per l'interessat.

En aquest sentit es pot considerar que la història social d'una persona es pot mantenir "activa" durant els cinc anys posteriors a la finalització de la prestació social corresponent. Transcorregut aquest temps es pot considerar que la història social és "passiva", i només s'hauria de mantenir si altres obligacions judicials o jurídiques així ho requereixin. En qualsevol cas, durant els períodes de conservació d'una història aquesta s'haurà de mantenir en l'arxiu central corresponent.

2.2.2. Deure d'informació

L'interessat ha de ser informat amb caràcter previ al tractament de les seves dades i de manera expressa, precisa e inequívoca del següent:

- De l'existència d'un fitxer o tractament de dades de caràcter personal.
- De la finalitat de la recollida d'aquestes.
- Dels destinataris de la informació.
- Del caràcter obligatori o facultatiu de les dades que es recullin.
- De les conseqüències de la obtenció de les dades o de la negativa a proporcionar-les.

- De la possibilitat d'exercir els drets d'accés, rectificació, cancel□lació i oposició.
- De la identitat i adreça del responsable del fitxer.

Pel que fa als casos en què les dades no són lliurades pel propi interessat, s'ha d'informar del tractament a l'afectat en un termini màxim de tres mesos.

El responsable del fitxer haurà d'acreditar que ha complert aquest deure i haurà de conservar mentre persisteixi el tractament el suport en el que consti el compliment.

2.2.3. Consentiment

Les dades de caràcter personal només podran ser objecte de tractament o cessió si l'interessat hagués donat prèviament el seu consentiment. El responsable del tractament serà l'encarregat de provar l'existència del consentiment.

Tot i que és recomanable obtenir-ne igualment el consentiment, aquest no és necessari en els següents supòsits:

- Quan les dades de caràcter personal es recullin per a l'exercici de les funcions pròpies de les Administracions Públiques en l'àmbit de les seves competències que li siguin atribuïdes per una norma amb rang de llei o de dret comunitari.
- Quan es refereixin a les parts d'un contracte o precontracte d'una relació de negoci, laboral o administrativa i siguin necessaris per al seu manteniment o compliment.
- Quan el tractament de les dades tingui per finalitat protegir un interès vital de l'interessat (salut).
- Quan les dades figurin en fonts accessibles al públic i el seu tractament sigui necessari per la satisfacció de l'interès legítim perseguit pel responsable del fitxer o per tercers a qui se li comuniquin les dades, sempre que no es vulnerin els drets i llibertats fonamentals de l'interessat.

La recomanació general és la de demanar sempre el consentiment per escrit a l'afectat, i en qualsevol cas serà obligatori fer-ho sempre que les dades es recullin per a alguna finalitat diferent a les que els supòsits mencionats es refereixin. Per exemple, si es recullen dades més enllà de les necessàries per a la prestació del servei social (és a dir, per a una altra finalitat) serà obligatori el consentiment del tractament per a aquesta finalitat.

Pel que fa al tractament o cessió de dades de menors, s'aplica el mateix criteri, però tenint en compte, a més:

- Per als menors de catorze anys cal el consentiment dels pares o tutors legals.
- Per als majors de catorze anys no caldrà aquest consentiment excepte en els casos en què la Llei ho exigeixi.

- Caldrà utilitzar un llenguatge clarament comprensible pel menor.
- Correspon al responsable del fitxer o tractament garantir que s'ha comprovat l'edat del menor i l'autenticitat dels pares o tutors, quan s'escaigui.

Excepte quan la llei exigeixi el consentiment explícit pel tractament de les dades, el responsable del tractament es podrà dirigir a l'afectat concedint-li un termini de 30 dies per a que manifesti la seva negativa, en cas de no fer-ho s'entendrà que dóna el consentiment. S'haurà de poder conèixer si la comunicació ha estat retornada.

S'entén que hi ha consentiment:

- Quan es signa un contracte i una de les clàusules informa sobre el tractament de dades de caràcter personal.
- Quan es complimenta un formulari i en el mateix s'informa mitjançant una clàusula o text.
- En el cas de les pàgines web, quan l'usuari envia les seves dades mitjançant un formulari, prement el botó d'enviar, i al costat hi ha un text (avís legal) en el que s'informa a l'usuari.

A més:

- Cal oferir un mitjà senzill i gratuït per a manifestar la negativa al tractament.
- Cal oferir un mitjà senzill i gratuït per a revocar el consentiment.

2.2.4. Dades especialment protegides

Es consideren dades especialment protegides les relatives a ideologia, afiliació sindical, religió o creences.

Per tractar aquestes dades cal el consentiment explícit i per escrit. A més, segons la Constitució ningú pot estar obligat a declarar sobre aquestes dades, per tant, existeix l'obligació d'advertir a l'interessat sobre el dret de no donar el seu consentiment.

2.2.5. Deure de secret

Els responsables de fitxers, els encarregats de tractaments i els usuaris tenen el deure de guardar secret professional respecte a les dades personals que coneguin com a conseqüència d'intervenir en el seu tractament, i a mantenir-lo fins i tot després de finalitzar les relacions amb el titular del fitxer.

En aquest sentit, es recomana la inclusió de clàusules específiques que hauran de signar tots els empleats públics, tinguin o no accés, a priori, a dades de caràcter personal. La signatura d'aquestes clàusules suposen una garantia formal del compliment del deure de secret dels responsables i encarregats del tractament i dels seus usuaris.

Addicionalment, hi ha altres ordenacions jurídiques que regulen el deure de secret de determinats col·lectius en la prestació de serveis socials, com per exemple:

- Article 95.1 de la Llei 6/1995, de 28 de Març, de garanties dels drets de la infància i l'adolescència, que estableix que els treballadors de serveis d'integració familiar tenen el deure de secret de tota la informació per a l'acolliment o l'adopció dels menors.
- Article 40 del Decret 147/2002, d'1 d'Agost, per el que s'aprova la renda mínima d'inserció social, segons el qual les Administracions Públiques tenen el deure de secret de les dades subministrades pels sol·licitants.

A més, les persones amb personal al seu càrrec, hauran de formar-les degudament en les seves funcions i obligacions respecte al tractament i protecció de dades de caràcter personal, especialment durant la fase d'acollida quan s'incorporin per primer cop als seus equips.

2.2.6. Drets de les persones

Els principals drets que tots els afectats tenen, fan referència a: l'accés, rectificació, cancel·lació de dades i oposició al seu tractament. La Llei configura aquest drets com drets independents, de forma que pugui entendre's que l'exercici de cap d'ells sigui requisit previ per l'exercici de l'altre.

Cal tenir en compte:

- Cal concedir a l'interessant un mitjà senzill i gratuït per a que exerceixi els seus drets.
- S'haurà d'atendre la sol·licitud encara que l'afectat no hagi utilitzat els mecanismes establerts a tal efecte.
- S'haurà de respondre la sol·licitud tant si figuren com si no dades de l'interessat en els seus fitxers.
- S'haurà de respondre la sol·licitud encara que no reuneixi els requisits necessaris, indicant aquest fet.
- S'haurà d'acreditar prova del compliment del deure de resposta, i conservar aquesta acreditació.

Per a l'exercici dels drets es recomana que en tots els centres d'Acció Social i dels possibles encarregats de tractament es disposi de models estàndard que facilitin la gestió.

<u>Dret d'accés</u>

L'interessat tindrà dret a sol·licitar i obtenir gratuïtament informació de les seves dades de caràcter personal incloses en els fitxers sotmesos a tractament, conèixer l'origen de les dades, així com les comunicacions realitzades o que es prevegi fer de

les mateixes.

La sol□licitud d'accés s'haurà de resoldre en un termini d'un mes a partir de la recepció de la mateixa.

En cas que la sol□licitud s'estimi i la informació no sigui acompanyada amb la comunicació de la resolució de la sol□licitud, es disposarà d'un termini de deu dies per a realitzar l'accés.

Rectificació i cancel□lació

Aquests drets atorguen la possibilitat a l'interessat d'exigir al responsable del fitxer que compleixi amb el principi de qualitat de les dades. Amb això s'assegura que les dades es mantinguin de forma adequada i no excessiva en relació a l'àmbit i finalitats legitimes per les quals es van recollir.

L'interessat té dret a que es rectifiquin aquelles dades de caràcter personal en les que el seu tractament no s'ajusta al que disposa la Llei i en particular, quan aquestes resultin inexactes o incompletes. També té dret a que es cancel□lin quan deixin de ser necessàries pel fi pel qual van ser enregistrades.

La sol□licitud de rectificació o cancel□lació s'haurà de resoldre en un termini de deu dies a partir de la recepció de la mateixa.

En cas que les dades haguessin estat cedides prèviament i la resolució fos favorable, el responsable del tractament disposarà de deu dies per comunicar al cessionari la resolució de la sol□licitud per a que aquest procedeixi a la seva vegada a la cancel□lació o rectificació de les dades.

Oposició

En els casos en els que el consentiment de l'afectat no sigui necessari pel tractament de les dades de caràcter personal i sempre que no hi hagi una Llei que digui el contrari, l'afectat podrà oposar-se al tractament de les dades si existeixen motius fonamentats i legítims relatius a una situació personal concreta.

La sol□licitud d'oposició s'haurà de resoldre en un termini de deu dies a partir de la recepció de la mateixa.

2.2.7. Document de Seguretat

El responsable del fitxer ha d'elaborar un document de seguretat que reculli les mesures tècniques i organitzatives, que serà d'obligat compliment per al personal amb accés a les dades de caràcter personal.

El document de seguretat pot ser únic per tots els fitxers o tractaments, individualitzat per fitxer o tractament, per sistema de tractament utilitzat o segons criteris organitzatius. És un document de caràcter intern de l'organització.

El document de seguretat s'ha de mantenir actualitzat i s'ha de revisar sempre que es produeixin canvis rellevants en el sistema d'informació, en la seva organització, en el sistema de tractament utilitzat, en el contingut de la informació inclosa en els fitxer, o

com a conseqüència dels controls periòdics realitzats. S'entendrà que un canvi es rellevant quan pugui repercutir en el compliment de les mesures de seguretat implantades.

El document de seguretat s'haurà d'adequar a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

2.2.8. Còpies de Treball

Els fitxers temporals o còpies de documents creats exclusivament per a la realització de treballs temporals o auxiliars, hauran de complir el nivell de seguretat que correspongui.

Tot fitxer temporal o còpia de treball serà esborrat o destruït un cop deixi de ser necessari per a la finalitat que va motivar la seva creació.

Cal evitar la realització de proves en sistemes d'informació amb dades reals, i en el cas que sigui necessari, caldrà també adoptar les mesures de seguretat aplicables al nivell que li correspongui.

2.3. Mesures de seguretat

2.3.1. Nivells de seguretat

Les mesures de seguretat a aplicar es divideixen en tres nivells: baix, mitjà i alt:

Nivell baix

Qualsevol fitxer amb dades de caràcter personal.

Nivell mig

Fitxers que continguin dades relatives a:

- Comissió d'infraccions administratives o penals.
- Prestació de serveis d'informació sobre solvència patrimonial i crèdit.
- Aquells dels quals siguin responsables administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries.
- Aquells dels quals en siguin responsables les entitats financeres per finalitats relacionades amb la prestació de serveis financers.
- Aquells que siguin responsabilitat de les Entitats Gestores i Serveis Comuns de la Seguretat Social i es relacionin amb l'exercici de les seves competències.
- Aquells dels quals en siguin responsables les mútues d'accidents de treball i malalties professionals de la Seguretat Social.
- Aquells que continguin un conjunt de dades que permetin fer una definició de les característiques o de la personalitat dels ciutadans, que permetin avaluar determinats aspectes de la seva personalitat o comportament.

Nivell alt

Fitxers que continguin dades relatives a:

- Ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
- Dades recollides per a finalitats policials sense consentiment de les persones afectades.
- Dades derivades d'actes de violència de gènere.

Les dades tractades per Acció Social són de **nivell alt**.

2.3.2. Quadre resum de mesures de seguretat

A continuació es mostra un quadre resum de les mesures de seguretat que cal aplicar als fitxers automatitzats, als manuals o a ambdós. Algunes de les mesures principals es troben detallades en els següents apartats.

Tipus de mesura	Nivell baix	Nivell mig	Nivell alt
Funcions i obligacions	TOTS ELS FITXERS		
Registre d'incidències (I)	TOTS ELS FITXERS		
Control d'accés	TOTS ELS FITXERS		
Gestió de suports i documents (I)	TOTS ELS FITXERS		
Criteris d'arxiu	FITXERS MANUALS		
Dispositius d'emmagatzemament	FITXERS MANUALS		
Custòdia de suports	FITXERS MANUALS		
Identificació i autenticació (I)	FITXERS AUTOMATITZATS		
Còpies de seguretat i recuperació	FITXERS AUTOMATITZATS		
Responsable de Seguretat	-	TOTS ELS FITXERS	
Auditoria	-	TOTS ELS FITXERS	
Gestió de suports i documents (II)	-	FITXERS AUTOMATITZATS	
Identificació i autenticació (II)	-	FITXERS AUTOMATITZATS	
Control d'accés físic	-	FITXERS AUTOMATITZATS	
Registre d'incidències (II)	-	FITXERS AUTOMATITZATS	
Emmagatzemament de la informació	-	-	FITXERS MANUALS
Còpia o reproducció	-	-	FITXERS MANUALS
Accés a la documentació	-	-	FITXERS MANUALS
Trasllat de documentació	-	-	FITXERS MANUALS
Gestió de suports i documents (III)	-	-	FITXERS AUTOMAT
Còpies de seguretat i recuperació (II)	.-	-	FITXERS AUTOMAT
Registre d'accessos	-	-	FITXERS AUTOMAT
Telecomunicacions	-	-	FITXERS AUTOMAT

2.3.3. Principals mesures comuns

Les següents mesures s'han d'aplicar a qualsevol fitxer o tractament:

Funcions i obligacions

Cal definir les funcions i obligacions que ha de complir tot el personal que tingui accés a les dades de caràcter personal:

- Les funcions i obligacions estaran documentades al Document de Seguretat.
- Es definiran les funcions de control pel responsable del fitxer o tractament.
- El responsable del fitxer farà difusió al personal afectat de forma comprensible les mesures de seguretat que afectin al desenvolupament de les seves funcions així com de les conseqüències en cas d'incompliment.

Registre d'incidències

Haurà d'existir un procediment de notificació i gestió de les incidències que afectin a les dades personals, i caldrà establir un registre en el que consti tipus d'incidència, moment en què s'ha produït o detectat, persona que notifica, a qui es comunica, efectes derivats i mesures correctores aplicades.

Control d'accés

Respecte a l'accés dels usuaris a les dades personals:

- L'usuari accedirà només a allò necessari pel desenvolupament de les seves funcions.
- El responsable del fitxer s'encarregarà que existeixi una relació actualitzada d'usuaris i perfils d'usuaris i accessos autoritzats.
- El responsable del fitxer establirà mecanismes que evitin accessos a dades o recursos amb drets diferents als autoritzats.
- El responsable del fitxer establirà criteris per la concessió de permisos d'accés i establirà el personal autoritzat a fer-ho.
- El personal aliè al responsable del fitxer amb accés als recursos haurà d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.

Gestió de suports i documents

Les següents mesures cal aplicar-les a qualsevol tipus de suport informatitzat i document que contingui dades de caràcter personal:

- Els suports i documents permetran identificar el tipus d'informació que contenen, ser inventariats i ser accessibles només a personal autoritzat,

excepte si les característiques físiques del suport no ho permeten. En aquest cas, ha de quedar constància al document de seguretat.

- La sortida de suports i documents amb dades personals fora dels locals sota el control del responsable del fitxer o tractament, inclosos els annexes a un correu electrònic, ha de ser autoritzada pel responsable del fitxer o estar degudament autoritzada al document de seguretat.
- Caldrà adoptar mesures per protegir la sostracció, pèrdua o accés indegut durant un trasllat.
- Caldrà adoptar mesures per impedir l'accés o la recuperació posterior d'informació d'un suport o document que vagi a ser destruït o esborrat.
- La identificació de suports amb dades personals considerades per la organització com especialment sensibles es podrà realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat que permetin als usuaris amb accés autoritzat identificar el seu contingut, i que dificultin la identificació per part d'altres persones.

2.3.4. Principals mesures en fitxers manuals

Les següents mesures s'han d'aplicar a fitxers o tractaments no automatitzats (manuals), o a aquells que siguin mixtes:

Dispositius d'emmagatzemament

Els dispositius d'emmagatzemament (arxivadors, calaixos, etc.), han de disposar de mecanismes que obstaculitzin l'obertura. Si els dispositius existents no permeten disposar d'aquests mecanismes, el Responsable del Fitxer adoptarà mesures alternatives per impedir l'accés no autoritzat.

Custòdia de suports

La persona a càrrec de documentació no arxivada, en procés de revisió o tramitació (per exemple, mentre es treballa en un expedient), prèviament o posteriorment al seu arxiu, és responsable de custodiar-la i impedir l'accés no autoritzat.

Emmagatzemament de la informació (només nivell alt)

Quan les dades siguin de nivell alt, caldrà adoptar mesures de protecció en les ubicacions on es trobin els calaixos, arxivadors, etc. on es trobi la documentació.

Els dispositius d'emmagatzemament hauran d'estar en àrees d'accés protegit amb portes d'accés dotades de sistemes d'obertura (clau o equivalent). Les àrees hauran d'estar tancades quan no sigui precís l'accés als documents.

Si per les característiques dels locals no és possible complir-ho, el Responsable del Fitxer adaptarà mesures alternatives, suficients i justificades, que s'inclouran al document de seguretat.

Còpia o reproducció (només nivell alt)

La còpia o reproducció de documents amb dades de nivell alt només és possible sota control del personal autoritzat al Document de Seguretat.

La destrucció de còpies o reproduccions que ja no es necessiten es farà garantint que no és possible accedir a la informació o la seva recuperació posterior, ja sigui amb destructores de paper o procediments similars, o amb l'ús de serveis d'empreses especialitzades.

Accés a la documentació (només nivell alt)

Cal aplicar mesures més restrictives per a identificar els accessos dels usuaris a dades de nivell alt:

- L'accés a la documentació estarà permès només a personal autoritzat.
- Caldrà establir mecanismes per identificar els accessos realitzats, si els documents poden ser utilitzats per múltiples usuaris.
- L'accés excepcional de persones no autoritzades, quedarà registrat segons el procediment establert en el Document de Seguretat.

Trasllat de documentació (només nivell alt)

Tot trasllat físic requerirà de l'aplicació de mesures que impedeixin l'accés o manipulació de la informació traslladada.

2.3.5. Principals mesures en fitxers automatitzats

Les següents mesures s'han d'aplicar a fitxers o tractaments automatitzats (informatitzats), o a aquells que siguin mixtes:

Identificació i autenticació

S'hauran d'establir procediments per a la identificació i autenticació d'accés als fitxers per part del personal, evitant així que es puguin produir accessos no autoritzats a les dades.

La identificació ha de ser inequívoca i personalitzada per a cada usuari que ha d'accedir a les dades, és a dir, no es poden utilitzar identificadors genèrics o compartits.

El mecanisme d'autenticació ha de garantir la verificació que l'usuari identificat té accés a les dades. En cas que es basi en contrasenyes, hi haurà d'haver un procediment d'assignació, distribució i emmagatzemament inintel□ligible que garanteixi la confidencialitat i integritat de les contrasenyes. A més aquestes hauran de canviar-se de forma periòdica, com a mínim anualment.

Addicionalment, per fitxers o tractaments de nivell mig o alt, s'haurà de limitar el nombre d'accessos reiterats d'accés no autoritzat, per exemple bloquejant l'usuari després d'un nombre determinat d'errors.

Gestió de suports (només alt)

Per fitxers o tractaments de nivell alt, caldrà:

- Identificar els suports amb sistemes d'etiquetatge comprensibles i amb significat (codificació), que permeti als usuaris autoritzats identificar contingut, dificultant la identificació per part d'altres persones.
- Fer la distribució de suports xifrant les dades o utilitzant qualsevol altre mecanisme que garanteixi que aquesta informació no sigui intel□ligible ni manipulable durant el seu transport.
- Xifrar les dades que continguin els dispositius portàtils quan aquests es trobin fora de les instal□lacions de tractament.

3. Guia de Bones Pràctiques i de Formació Avançada als Responsables

Aquest capítol va adreçat als caps i responsables de departaments, àrees o serveis, i al personal amb responsabilitat en el tractament de dades de caràcter personal.

L'objectiu d'aquesta guia és oferir una idea general de la Llei Orgànica de Protecció de Dades (LOPD), els seus principis bàsics, els drets i deures, les mesures de seguretat que cal aplicar sobre les dades de caràcter personal (DCP) i les funcions i obligacions de les persones.

3.1. Introducció a la Protecció de dades

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (des d'ara LOPD) té per objecte, garantir i protegir, en el que concerneix al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i intimitat personal i familiar.

La protecció de les dades personals és un dret fonamental que afecta a qualsevol tipus de dada, sigui íntima o no, i com a tal és irrenunciable i preval sobre qualsevol altre dret.

L'aplicació de la LOPD en el sector dels Serveis Socials té diverses particularitats:

- Les dades de caràcter personal tractades són molt sensibles.
- És habitual que les dades es cedeixin o comuniquin de forma legítima a altres Administracions Públiques.
- Els fluxos de dades en paper són habituals, fet que en dificulta el control i la custodia.
- Existeix una elevada deslocalització geogràfica de la xarxa de centres socials.
- És habitual que la tramitació administrativa la realitzin terceres persones en nom dels afectats o beneficiaris dels serveis.
- Existeixen nombrosos serveis concertats o externalitzats.

3.1.1. Normativa aplicable

A fi de garantir la necessària seguretat jurídica en un àmbit tan sensible per als drets fonamentals dels ciutadans com és el de la protecció de dades, existeix un legislació complexa d'obligat compliment tant per al sector públic com privat entre la qual destaquen:

- Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.
- Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

Altra normativa destacable:

- Article 18.4 de la Constitució Espanyola.
- Conveni Europeu per a la protecció de les persones amb respecte al tractament automatitzat de dades de caràcter personal, de 28 de Gener de 1981.
- Directiva 95/46/CE, del Parlament Europeu i del Consell, de 24 d'octubre de 1995 relativa a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades (DOCE L 281 de 23.11.1995).
- Sentència 292/2000, de 30 de novembre de 2000 del Tribunal Constitucional.
- Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades (DOGC núm. 3625 de 29.4.2002).
- Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades (DOGC núm. 3835 de 4.3.2003).
- Resolució de 23 de juny de 2004, per la qual es modifiquen els suports normalitzats de les sol□licituds d'inscripció al Registre de protecció de dades de Catalunya.
- Llei Orgànica 6/2006, de 19 de juliol, de reforma de l'Estatut d'Autonomia de Catalunya publicada pel Decret 306/2006, de 20 de juliol de 2006. Article 31 i 156.

3.1.2. Definicions

Dades de caràcter personal: Qualsevol informació concernent a persones físiques identificades o identificables.

Tractament de dades: qualsevol operació o procediment de caràcter automatitzat o no que s'apliqui a dades personals.

Fitxer de dades personals: qualsevol conjunt estructurat de dades personals, independentment de la seva modalitat de creació, emmagatzemament, organització i accés.

Comunicació o cessió: tota revelació de dades personals feta a una persona diferent de l'interessat.

Afectat o interessat: persona física titular de les dades que siguin objecte de tractament.

Responsable del fitxer: persona física o jurídica, pública o privada, o òrgan administratiu o unitat funcional que decideixi sobre la finalitat, contingut, ús i tractament de dades personals.

Encarregat del tractament: aquella persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, individualment o conjuntament amb d'altres, tracti dades personals per compte del responsable del fitxer.

Usuari: qualsevol persona física o procés autoritzat a accedir a dades o recursos.

3.1.3. Àmbit d'aplicació

Dades de caràcter personal registrades en suport físic, que les faci susceptibles de tractament, i tota modalitat d'ús posterior d'aquestes dades pels sectors públic i privat.

No aplica a:

- Fitxers mantinguts per persones físiques en l'àmbit exclusivament personal o domèstic.
- Fitxers sotmesos a la normativa sobre protecció de matèries classificades.
- Fitxers establerts per a investigacions del terrorisme i delinqüència organitzada.

3.1.4. Agència Catalana de Protecció de Dades

L'Agència Catalana de Protecció de Dades (en endavant, APDCat) exerceix les competències de registre, inspecció, sanció i resolució, així com l'emissió de recomanacions i instruccions, en l'àmbit dels fitxers de dades de caràcter personal de:

- La Generalitat de Catalunya
- Els Ajuntaments i ens de l'Administració local
- Les universitats catalanes
- Els organismes i entitats que depenen de les administracions públiques catalanes i els consorcis dels quals formen part

Els fitxers de dades de caràcter personal en aquest àmbit s'inscriuen en l'APDCat, qui s'encarrega de notificar-los al Registre General de Protecció de Dades.

3.1.5. Procediment de notificació

Per tal de crear/modificar/suprimir un fitxer amb dades de caràcter personal cal comunicar-ho a Informació de Base i Cartografia (IBC), usant el procediment que es troba en l'ANNEX III d'aquest document.

A partir d'aleshores els tràmits que s'executen són els següents:

- IBC prepara informe favorable.
- El Sector corresponent demana informe jurídic.
- El Sector fa l'expedient necessari per la publicació en el BOP del Decret d'Aprovació Provisional (20 dies hàbils).
- El Sector publica al BOP el Decret d'Aprovació definitiva i comunica el núm. de BOP a IBC.
- IBC realitza la notificació a l'APDCat.
- L'APDCat notifica al Registre General de Protecció de Dades.

3.2. Principis de protecció de dades

3.2.1. Qualitat de les dades

Les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut.

Per tant:

- Cal definir inicialment la finalitat per a la qual es vol recollir les dades.
- No es poden utilitzar les dades per a una finalitat diferent a aquesta.
- No s'han de recollir dades que no siguin necessàries per a aquesta finalitat.
- Les dades han de ser exactes i veraces, en cas contrari s'han de cancel·lar i substituir d'ofici.

Les dades personals han de ser cancel·lades un cop deixin de ser necessàries o pertinents per la finalitat per la qual havien estat recollides. No obstant, es podran conservar durant el temps en què es pugui exigir algun tipus de responsabilitat derivada de:

- Una relació o obligació jurídica,
- l'execució d'un contracte, o bé
- l'aplicació de mesures pre-contractuals sol·licitades per l'interessat.

En aquest sentit es pot considerar que la història social d'una persona es pot mantenir "activa" durant els cinc anys posteriors a la finalització de la prestació social corresponent. Transcorregut aquest temps es pot considerar que la història social és "passiva", i només s'hauria de mantenir si altres obligacions judicials o jurídiques així ho requereixin. En qualsevol cas, durant els períodes de conservació d'una història aquesta s'haurà de mantenir en l'arxiu central corresponent.

3.2.2. Deure d'informació

L'interessat ha de ser informat amb caràcter previ al tractament de les seves dades i de manera expressa, precisa e inequívoca del següent:

- De l'existència d'un fitxer o tractament de dades de caràcter personal.
- De la finalitat de la recollida d'aquestes.
- Dels destinataris de la informació.
- Del caràcter obligatori o facultatiu de les dades que es recullin.
- De les conseqüències de la obtenció de les dades o de la negativa a proporcionar-les.

- De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
- De la identitat i adreça del responsable del fitxer.

Pel que fa als casos en què les dades no són lliurades pel propi interessat, s'ha d'informar del tractament a l'afectat en un termini màxim de tres mesos.

El responsable del fitxer haurà d'acreditar que ha complert aquest deure i haurà de conservar mentre persisteixi el tractament el suport en el que consti el compliment.

3.2.3. Consentiment

Les dades de caràcter personal només podran ser objecte de tractament o cessió si l'interessat hagués donat prèviament el seu consentiment. El responsable del tractament serà l'encarregat de provar l'existència del consentiment.

Tot i que és recomanable obtenir-ne igualment el consentiment, aquest no és necessari en els següents supòsits:

- Quan les dades de caràcter personal es recullin per a l'exercici de les funcions pròpies de les Administracions Públiques en l'àmbit de les seves competències que li siguin atribuïdes per una norma amb rang de llei o de dret comunitari.
- Quan es refereixin a les parts d'un contracte o precontracte d'una relació de negoci, laboral o administrativa i siguin necessaris per al seu manteniment o compliment.
- Quan el tractament de les dades tingui per finalitat protegir un interès vital de l'interessat (salut).
- Quan les dades figurin en fonts accessibles al públic i el seu tractament sigui necessari per la satisfacció de l'interès legítim perseguit pel responsable del fitxer o per tercers a qui se li comuniquin les dades, sempre que no es vulnerin els drets i llibertats fonamentals de l'interessat.

La recomanació general és la de demanar sempre el consentiment per escrit a l'afectat, i en qualsevol cas serà obligatori fer-ho sempre que les dades es recullin per a alguna finalitat diferent a les que els supòsits mencionats es refereixin. Per exemple, si es recullen dades més enllà de les necessàries per a la prestació del servei social (és a dir, per a una altra finalitat) serà obligatori el consentiment del tractament per a aquesta finalitat.

Pel que fa al tractament o cessió de dades de menors, s'aplica el mateix criteri, però tenint en compte, a més:

- Per als menors de catorze anys cal el consentiment dels pares o tutors legals.
- Per als majors de catorze anys no caldrà aquest consentiment excepte en els casos en què la Llei ho exigeixi.

- Caldrà utilitzar un llenguatge clarament comprensible pel menor.
- Correspon al responsable del fitxer o tractament garantir que s'ha comprovat l'edat del menor i l'autenticitat dels pares o tutors, quan s'escaigui.

Excepte quan la llei exigeixi el consentiment explícit pel tractament de les dades, el responsable del tractament es podrà dirigir a l'afectat concedint-li un termini de 30 dies per a que manifesti la seva negativa, en cas de no fer-ho s'entendrà que dóna el consentiment. S'haurà de poder conèixer si la comunicació ha estat retornada.

S'entén que hi ha consentiment:

- Quan es signa un contracte i una de les clàusules informa sobre el tractament de dades de caràcter personal.
- Quan es complimenta un formulari i en el mateix s'informa mitjançant una clàusula o text.
- En el cas de les pàgines web, quan l'usuari envia les seves dades mitjançant un formulari, prement el botó d'enviar, i al costat hi ha un text (avís legal) en el que s'informa a l'usuari.

A més:

- Cal oferir un mitjà senzill i gratuït per a manifestar la negativa al tractament.
- Cal oferir un mitjà senzill i gratuït per a revocar el consentiment.

3.2.4. Dades especialment protegides

Es consideren dades especialment protegides les relatives a ideologia, afiliació sindical, religió o creences.

Per tractar aquestes dades cal el consentiment explícit i per escrit. A més, segons la Constitució ningú pot estar obligat a declarar sobre aquestes dades, per tant, existeix l'obligació d'advertir a l'interessat sobre el dret de no donar el seu consentiment.

3.2.5. Deure de secret

Els responsables de fitxers, els encarregats de tractaments i els usuaris tenen el deure de guardar secret professional respecte a les dades personals que coneguin com a conseqüència d'intervenir en el seu tractament, i a mantenir-lo fins i tot després de finalitzar les relacions amb el titular del fitxer.

En aquest sentit, es recomana la inclusió de clàusules específiques que hauran de signar tots els empleats públics, tinguin o no accés, a priori, a dades de caràcter personal. La signatura d'aquestes clàusules suposen una garantia formal del compliment del deure de secret dels responsables i encarregats del tractament i dels seus usuaris.

Addicionalment, hi ha altres ordenacions jurídiques que regulen el deure de secret de determinats col·lectius en la prestació de serveis socials, com per exemple:

- Article 95.1 de la Llei 6/1995, de 28 de Març, de garanties dels drets de la infància i l'adolescència, que estableix que els treballadors de serveis d'integració familiar tenen el deure de secret de tota la informació per a l'acolliment o l'adopció dels menors.
- Article 40 del Decret 147/2002, d'1 d'Agost, per el que s'aprova la renda mínima d'inserció social, segons el qual les Administracions Públiques tenen el deure de secret de les dades subministrades pels sol·licitants.

A més, les persones amb personal al seu càrrec, hauran de formar-les degudament en les seves funcions i obligacions respecte al tractament i protecció de dades de caràcter personal, especialment durant la fase d'acollida quan s'incorporin per primer cop als seus equips.

3.2.6. Prestació de serveis

L'accés a les dades de caràcter personal per part d'un encarregat del tractament (contractista) no es considerarà cessió quan aquest sigui necessari per la prestació d'un servei al responsable del tractament (Ajuntament de Barcelona). Aquest servei podrà tenir o no un caràcter remunerat i podrà ser temporal o indefinit.

La prestació del servei haurà d'estar regulada en un contracte per escrit o per algun altre mitjà que permeti garantir la seva celebració i contingut, fent-se constar explícitament:

- L'encarregat del tractament només podrà tractar les dades per a la finalitat que figura al contracte, i no les comunicarà a tercers ni per la seva conservació sense la indicació expressa del responsable.
- Les mesures de seguretat que l'encarregat està obligat a implementar.
- Les dades hauran de ser retornades o destruïdes, així com qualsevol suport o document objecte del tractament, un cop s'hagi finalitzat la prestació contractual.
- En cas que l'encarregat destini les dades a una altra finalitat, les comuniqui a un tercer, o les utilitzi incomplint les estipulacions del contracte serà considerat responsable del tractament i respondrà com a tal de les infraccions que hagués incorregut personalment.

Aquesta situació és d'aplicació també en el cas que per alguns dels serveis s'hagi contractat a treballadors autònoms, ja que aquests també son considerats encarregats del tractament.

El responsable haurà de vetllar per a que l'encarregat reuneixi les garanties per al compliment de la normativa en vigor.

Pel que fa a la prestació de serveis sense accés a dades de caràcter personal, com ara en els casos de serveis de neteja o de seguretat, igualment es recomana que en el contracte es reculli la prohibició d'accedir a les dades personals i l'obligació de secret respecte de les dades que el personal pogués conèixer.

3.2.7. Drets de les persones

Els principals drets que tots els afectats tenen, fan referència a: l'accés, rectificació, cancel□lació de dades i oposició al seu tractament. La Llei configura aquest drets com drets independents, de forma que pugui entendre's que l'exercici de cap d'ells sigui requisit previ per l'exercici de l'altre.

Cal tenir en compte:

- Cal concedir a l'interessant un mitjà senzill i gratuït per a que exerceixi els seus drets.
- S'haurà d'atendre la sol□licitud encara que l'afectat no hagi utilitzat els mecanismes establerts a tal efecte.
- S'haurà de respondre la sol□licitud tant si figuren com si no dades de l'interessat en els seus fitxers.
- S'haurà de respondre la sol□licitud encara que no reuneixi els requisits necessaris, indicant aquest fet.
- S'haurà d'acreditar prova del compliment del deure de resposta, i conservar aquesta acreditació.

Per a l'exercici dels drets es recomana que en tots els centres d'Acció Social i dels possibles encarregats de tractament es disposi de models estàndard que facilitin la gestió.

Dret d'accés

L'interessat tindrà dret a sol□licitar i obtenir gratuïtament informació de les seves dades de caràcter personal incloses en els fitxers sotmesos a tractament, conèixer l'origen de les dades, així com les comunicacions realitzades o que es prevegi fer de les mateixes.

La sol□licitud d'accés s'haurà de resoldre en un termini d'un mes a partir de la recepció de la mateixa.

En cas que la sol□licitud s'estimi i la informació no sigui acompanyada amb la comunicació de la resolució de la sol□licitud, es disposarà d'un termini de deu dies per a realitzar l'accés.

Rectificació i cancel□lació

Aquests drets atorguen la possibilitat a l'interessat d'exigir al responsable del fitxer que compleixi amb el principi de qualitat de les dades. Amb això s'assegura que les dades es mantinguin de forma adequada i no excessiva en relació a l'àmbit i finalitats legitimes per les quals es van recollir.

L'interessat té dret a que es rectifiquin aquelles dades de caràcter personal en les que el seu tractament no s'ajusta al que disposa la Llei i en particular, quan aquestes resultin inexactes o incompletes. També té dret a que es cancel□lin quan deixin de ser necessàries pel fi pel qual van ser enregistrades.

La sol□licitud de rectificació o cancel□lació s'haurà de resoldre en un termini de deu dies a partir de la recepció de la mateixa.

En cas que les dades haguessin estat cedides prèviament i la resolució fos favorable, el responsable del tractament disposarà de deu dies per comunicar al cessionari la resolució de la sol□licitud per a que aquest procedeixi a la seva vegada a la cancel□lació o rectificació de les dades.

Oposició

En els casos en els que el consentiment de l'afectat no sigui necessari pel tractament de les dades de caràcter personal i sempre que no hi hagi una Llei que digui el contrari, l'afectat podrà oposar-se al tractament de les dades si existeixen motius fonamentats i legítims relatius a una situació personal concreta.

La sol□licitud d'oposició s'haurà de resoldre en un termini de deu dies a partir de la recepció de la mateixa.

3.2.8. Document de Seguretat

El responsable del fitxer ha d'elaborar un document de seguretat que reculli les mesures tècniques i organitzatives, que serà d'obligat compliment per al personal amb accés a les dades de caràcter personal.

El document de seguretat pot ser únic per tots els fitxers o tractaments, individualitzat per fitxer o tractament, per sistema de tractament utilitzat o segons criteris organitzatius. És un document de caràcter intern de l'organització.

L'estructura bàsica i contingut del document de seguretat és:

- Àmbit d'aplicació, amb especificació detallada dels recursos protegits.
- Mesures, normes, procediments d'actuació, regles i estàndards que garanteixen el nivell de seguretat exigit.
- Funcions i obligacions del personal en relació amb el tractament de les dades de caràcter personal.
- Estructura dels fitxers i descripció dels sistemes d'informació que els tracten.
- Procediment de notificació, gestió i resposta davant incidències.
- Procediments de còpies de seguretat i recuperació de dades pels fitxers

automatitzats.

- Mesures pel transport de suports i documents, així com per la seva destrucció o reutilització.
- Per els fitxers de nivell mig o alt, la Identificació del responsable o responsables de seguretat.
- Per els fitxers de nivell mig o alt, els controls periòdics (auditoria) que s'han de realitzar per verificar el compliment del que es disposa en el propi document.
- Si existeix tractament de dades per compte de tercers, la identificació dels fitxers o tractaments que haurà de tractar l'encarregat amb referència expressa al contracte o document que regula les condicions de l'encàrrec, identificació del responsable i període de vigència de l'encàrrec.

Quan les dades personals d'un fitxer o tractament s'incorporin i tractin de forma exclusiva en els sistemes de l'encarregat, s'haurà de fer constar al document de seguretat. En aquest cas, es podrà delegar la realització i manteniment del document de seguretat en l'encarregat del tractament, fent-ho constar en el contracte celebrat especificant els fitxers afectats.

El document de seguretat s'ha de mantenir actualitzat i s'ha de revisar sempre que es produeixin canvis rellevants en el sistema d'informació, en la seva organització, en el sistema de tractament utilitzat, en el contingut de la informació inclosa en els fitxer, o com a conseqüència dels controls periòdics realitzats. S'entendrà que un canvi es rellevant quan pugui repercutir en el compliment de les mesures de seguretat implantades.

El document de seguretat s'haurà d'adequar a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

3.2.9. Còpies de Treball

Els fitxers temporals o còpies de documents creats exclusivament per a la realització de treballs temporals o auxiliars, hauran de complir el nivell de seguretat que correspongui.

Tot fitxer temporal o còpia de treball serà esborrat o destruït un cop deixi de ser necessari per a la finalitat que va motivar la seva creació.

Cal evitar la realització de proves en sistemes d'informació amb dades reals, i en el cas que sigui necessari, caldrà també adoptar les mesures de seguretat aplicables al nivell que li correspongui.

3.3. Mesures de seguretat

3.3.1. Nivells de seguretat

Les mesures de seguretat a aplicar es divideixen en tres nivells: baix, mitjà i alt:

Nivell baix

Qualsevol fitxer amb dades de caràcter personal.

Nivell mig

Fitxers que continguin dades relatives a:

- Comissió d'infraccions administratives o penals.
- Prestació de serveis d'informació sobre solvència patrimonial i crèdit.
- Aquells dels quals siguin responsables administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries.
- Aquells dels quals en siguin responsables les entitats financeres per finalitats relacionades amb la prestació de serveis financers.
- Aquells que siguin responsabilitat de les Entitats Gestores i Serveis Comuns de la Seguretat Social i es relacionin amb l'exercici de les seves competències.
- Aquells dels quals en siguin responsables les mútues d'accidents de treball i malalties professionals de la Seguretat Social.
- Aquells que continguin un conjunt de dades que permetin fer una definició de les característiques o de la personalitat dels ciutadans, que permetin avaluar determinats aspectes de la seva personalitat o comportament.

Nivell alt

Fitxers que continguin dades relatives a:

- Ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
- Dades recollides per a finalitats policials sense consentiment de les persones afectades.
- Dades derivades d'actes de violència de gènere.

3.3.2. Aplicació dels nivells de seguretat

Les mesures de seguretat que cal aplicar a un fitxer són en funció dels nivells descrits, i són acumulables: als fitxers de nivell alt cal també aplicar les dels nivells mig i baix, i als de nivell mig, incorporar les de nivell baix.

Excepcions:

- Fitxers dels quals en siguin responsables els operadors que presten serveis de comunicacions electròniques disponibles al públic, o exploten xarxes públiques de comunicacions electròniques respecte les dades de tràfic i dades de localització. S'aplicaran mesures de nivell baix i mig, i les mesures de registre d'accés exigibles pel nivell alt.
- Fitxers que continguin dades de ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual, s'aplicaran mesures de nivell baix quan:
  - Les dades s'utilitzin amb l'única finalitat de realitzar una transferència dinerària a les entitats de les quals els afectats siguin associats o membres.
  - Es tracti de fitxers o tractaments no automatitzats que de forma incidental continguin dades d'aquesta tipologia sense guardar relació amb la seva finalitat.
- S'aplicaran mesures de nivell baix en fitxers o tractaments que continguin dades de salut, referents exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'afectat, amb motiu del compliment dels deures públics.

3.3.3. Quadre resum de mesures de seguretat

A continuació es mostra un quadre resum de les mesures de seguretat que cal aplicar als fitxers automatitzats, als manuals o a ambdós. Les mesures es troben detallades en els següents apartats.

Tipus de mesura	Nivell baix	Nivell mig	Nivell alt
Funcions i obligacions	TOTS ELS FITXERS		
Registre d'incidències (I)	TOTS ELS FITXERS		
Control d'accés	TOTS ELS FITXERS		
Gestió de suports i documents (I)	TOTS ELS FITXERS		
Criteris d'arxiu	FITXERS MANUALS		
Dispositius d'emmagatzemament	FITXERS MANUALS		
Custòdia de suports	FITXERS MANUALS		
Identificació i autenticació (I)	FITXERS AUTOMATITZATS		
Còpies de seguretat i recuperació	FITXERS AUTOMATITZATS		

Tipus de mesura	Nivell baix	Nivell mig	Nivell alt
Responsable de Seguretat	-	TOTS ELS FITXERS	
Auditoria	-	TOTS ELS FITXERS	
Gestió de suports i documents (II)	-	FITXERS AUTOMATITZATS	
Identificació i autenticació (II)	-	FITXERS AUTOMATITZATS	
Control d'accés físic	-	FITXERS AUTOMATITZATS	
Registre d'incidències (II)	-	FITXERS AUTOMATITZATS	
Emmagatzemament de la informació	-	-	FITXERS MANUALS
Còpia o reproducció	-	-	FITXERS MANUALS
Accés a la documentació	-	-	FITXERS MANUALS
Trasllat de documentació	-	-	FITXERS MANUALS
Gestió de suports i documents (III)	-	-	FITXERS AUTOMAT
Còpies de seguretat i recuperació (II)	.-	-	FITXERS AUTOMAT
Registre d'accessos	-	-	FITXERS AUTOMAT
Telecomunicacions	-	-	FITXERS AUTOMAT

3.3.4. Mesures comuns

Les següents mesures s'han d'aplicar a qualsevol fitxer o tractament:

Funcions i obligacions

Cal definir les funcions i obligacions que ha de complir tot el personal que tingui accés a les dades de caràcter personal:

- Les funcions i obligacions estaran documentades al Document de Seguretat.
- Es definiran les funcions de control pel responsable del fitxer o tractament.
- El responsable del fitxer farà difusió al personal afectat de forma comprensible les mesures de seguretat que afectin al desenvolupament de les seves funcions així com de les conseqüències en cas d'incompliment.

Registre d'incidències

Haurà d'existir un procediment de notificació i gestió de les incidències que afectin a les dades personals, i caldrà establir un registre en el que consti tipus d'incidència, moment en què s'ha produït o detectat, persona que notifica, a qui es comunica, efectes derivats i mesures correctores aplicades.

Control d'accés

Respecte a l'accés dels usuaris a les dades personals:

- L'usuari accedirà només a allò necessari pel desenvolupament de les seves funcions.
- El responsable del fitxer s'encarregarà que existeixi una relació actualitzada d'usuaris i perfils d'usuaris i accessos autoritzats.
- El responsable del fitxer establirà mecanismes que evitin accessos a dades o recursos amb drets diferents als autoritzats.
- El responsable del fitxer establirà criteris per la concessió de permisos d'accés i establirà el personal autoritzat a fer-ho.
- El personal aliè al responsable del fitxer amb accés als recursos haurà d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.

Gestió de suports i documents

Les següents mesures cal aplicar-les a qualsevol tipus de suport informatitzat i document que contingui dades de caràcter personal:

- Els suports i documents permetran identificar el tipus d'informació que contenen, ser inventariats i ser accessibles només a personal autoritzat, excepte si les característiques físiques del suport no ho permeten. En aquest cas, ha de quedar constància al document de seguretat.
- La sortida de suports i documents amb dades personals fora dels locals sota el control del responsable del fitxer o tractament, inclosos els annexes a un correu electrònic, ha de ser autoritzada pel responsable del fitxer o estar degudament autoritzada al document de seguretat.
- Caldrà adoptar mesures per protegir la sostracció, pèrdua o accés indegut durant un trasllat.
- Caldrà adoptar mesures per impedir l'accés o la recuperació posterior d'informació d'un suport o document que vagi a ser destruït o esborrat.
- La identificació de suports amb dades personals considerades per la organització com especialment sensibles es podrà realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat que permetin als usuaris amb accés autoritzat identificar el seu contingut, i que dificultin la identificació per part d'altres persones.

Responsable de seguretat (només nivell mig i alt)

Es designarà un o més responsables de seguretat que s'encarregaran de coordinar i controlar les mesures de seguretat. La designació pot ser única o diferenciada per fitxers o tractaments, fent-se constar clarament al document de seguretat.

Auditoria (només nivell mig i alt)

Cal realitzar una auditoria, mínim cada dos anys, interna o externa, per verificar el compliment de les mesures de seguretat.

3.3.5. Mesures en fitxers manuals

Les següents mesures s'han d'aplicar a fitxers o tractaments no automatitzats (manuals), o a aquells que siguin mixtes:

Criteris d'arxiu

L'arxiu de documents i suports es farà segons els criteris definits pel Responsable del Fitxer, per tal de garantir la correcta conservació dels documents, localització i consulta, i per a possibilitar l'exercici de drets d'accés, rectificació, cancel□lació i oposició.

Dispositius d'emmagatzemament

Els dispositius d'emmagatzemament (arxivadors, calaixos, etc.), han de disposar de mecanismes que obstaculitzin l'obertura. Si els dispositius existents no permeten disposar d'aquests mecanismes, el Responsable del Fitxer adoptarà mesures alternatives per impedir l'accés no autoritzat.

Custòdia de suports

La persona a càrrec de documentació no arxivada, en procés de revisió o tramitació (per exemple, mentre es treballa en un expedient), prèviament o posteriorment al seu arxiu, és responsable de custodiar-la i impedir l'accés no autoritzat.

Emmagatzemament de la informació (només nivell alt)

Quan les dades siguin de nivell alt, caldrà adoptar mesures de protecció en les ubicacions on es trobin els calaixos, arxivadors, etc. on es trobi la documentació.

Els dispositius d'emmagatzemament hauran d'estar en àrees d'accés protegit amb portes d'accés dotades de sistemes d'obertura (clau o equivalent). Les àrees hauran d'estar tancades quan no sigui precís l'accés als documents.

Si per les característiques dels locals no és possible complir-ho, el Responsable del Fitxer adaptarà mesures alternatives, suficients i justificades, que s'inclouran al document de seguretat.

Còpia o reproducció (només nivell alt)

La còpia o reproducció de documents amb dades de nivell alt només és possible sota control del personal autoritzat al Document de Seguretat.

La destrucció de còpies o reproduccions que ja no es necessiten es farà garantint que no és possible accedir a la informació o la seva recuperació posterior, ja sigui amb destructores de paper o procediments similars, o amb l'ús de serveis d'empreses especialitzades.

Accés a la documentació (només nivell alt)

Cal aplicar mesures més restrictives per a identificar els accessos dels usuaris a dades de nivell alt:

- L'accés a la documentació estarà permès només a personal autoritzat.
- Caldrà establir mecanismes per identificar els accessos realitzats, si els documents poden ser utilitzats per múltiples usuaris.
- L'accés excepcional de persones no autoritzades, quedarà registrat segons el procediment establert en el Document de Seguretat.

Trasllat de documentació (només nivell alt)

Tot trasllat físic requerirà de l'aplicació de mesures que impedeixin l'accés o manipulació de la informació traslladada.

3.3.6. Mesures en fitxers automatitzats

Les següents mesures s'han d'aplicar a fitxers o tractaments automatitzats (informatitzats), o a aquells que siguin mixtes:

Identificació i autenticació

S'hauran d'establir procediments per a la identificació i autenticació d'accés als fitxers per part del personal, evitant així que es puguin produir accessos no autoritzats a les dades.

La identificació ha de ser inequívoca i personalitzada per a cada usuari que ha d'accedir a les dades, és a dir, no es poden utilitzar identificadors genèrics o compartits.

El mecanisme d'autenticació ha de garantir la verificació que l'usuari identificat té accés a les dades. En cas que es basi en contrasenyes, hi haurà d'haver un procediment d'assignació, distribució i emmagatzemament inintel□ligible que

garanteixi la confidencialitat i integritat de les contrasenyes. A més aquestes hauran de canviar-se de forma periòdica, com a mínim anualment.

Addicionalment, per fitxers o tractaments de nivell mig o alt, s'haurà de limitar el nombre d'accessos reiterats d'accés no autoritzat, per exemple bloquejant l'usuari després d'un nombre determinat d'errors.

Còpies de seguretat i restauració

S'han de fer còpies de seguretat, com a mínim setmanalment, llevat que en aquest període no s'hagi produït cap actualització de les dades. Els procediments establerts per fer còpies de seguretat i per recuperar les dades han de garantir-ne la reconstrucció a l'estat en què estaven en el moment de produir-se la pèrdua o la destrucció.

Cada sis mesos, com a mínim. cal verificar la definició i aplicació dels procediments de còpia i restauració, així com verificar-ne el correcte funcionament.

Addicionalment, per fitxers o tractaments de nivell alt, s'ha de conservar mínim una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent d'aquell on es troben els equips informàtics que els tracten i complir, en tot cas, les mesures de seguretat del fitxer.

Gestió de suports (només nivell mig i alt)

S'ha d'establir un sistema de registre d'entrada i sortida de suports informàtics que permeti conèixer:

- Tipus de suport,
- data i l'hora d'entrada o sortida,
- emissor i receptor,
- nombre de suports,
- tipus d'informació que contenen, i
- forma d'enviament

Addicionalment, per fitxers o tractaments de nivell alt, caldrà:

- Identificar els suports amb sistemes d'etiquetatge comprensibles i amb significat (codificació), que permeti als usuaris autoritzats identificar contingut, dificultant la identificació per part d'altres persones.
- Fer la distribució de suports xifrant les dades o utilitzant qualsevol altre mecanisme que garanteixi que aquesta informació no sigui intel□ligible ni manipulable durant el seu transport.

- Xifrar les dades que continguin els dispositius portàtils quan aquests es trobin fora de les instal·lacions de tractament.

Control d'accés físic (només nivell mig i alt)

S'haurà de restringir l'accés físic als locals on es trobin ubicats els sistemes d'informació al personal autoritzat i identificat en el document de seguretat.

Registre d'incidències (només nivell mig i alt)

En el registre d'incidències també cal incloure:

- L'execució de procediments de restauració que es produeixin.
- La persona que va executar el procés.
- L'autorització per escrit del responsable del fitxer per fer la recuperació.
- Les dades restaurades i les que hagi calgut gravar manualment (si s'escau)

Registre d'accessos (només nivell alt)

S'haurà de mantenir un registre de tots els accessos als fitxers amb dades de caràcter personal, que guardarà:

- Identificació de l'usuari
- Data i hora
- Fitxer accedit
- Tipus d'accés
- Accés autoritzat o denegat
- La informació que permeti identificar les dades accedides, sempre i quan l'accés hagi estat autoritzat

El responsable del fitxer haurà de posar mecanismes per tal de garantir que:

- El registre es conserva, com a mínim, durant dos anys.
- Mai es permetrà la desactivació o manipulació del registre
- Es revisa el registre, com a mínim cada mes, s'elabora un informe d'aquestes revisions i dels problemes detectats

Telecomunicacions (només nivell alt)

La transmissió de dades de caràcter personal mitjançant xarxes de telecomunicacions públiques o a través de qualsevol xarxa sense fils (encara que sigui privada) es realitzarà xifrant les dades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulable per tercers.

4. Guia de Desenvolupament d'Aplicacions

Aquest capítol va adreçat als gestors de projecte dels diferents organismes, gestors funcionals, analistes i programadors interns i/o externs.

L'objectiu d'aquesta guia és orientar sobre els requeriments i controls de seguretat que cal implementar en les aplicacions que tracten dades de caràcter personal de **nivell alt** segons les exigències de la normativa de protecció de dades vigent.

4.1. Definició i verificació dels requeriments previs

Prèviament al desenvolupament de l'aplicació, caldrà verificar que s'hagin complert les mesures legals i organitzatives pertinents.

4.1.1. Requeriments previs: mesures legals i organitzatives

L'organisme responsable de la elaboració de l'aplicació o del tractament de dades haurà de comprovar la següent llista de verificació:

ID	Control	Comentaris
I.1	Comprovar que les dades que tracta l'aplicació formen part d'un fitxer o tractament ja declarat.	
I.2	Informar al Responsable de Seguretat per a que actualitzi, si s'escau, el document de seguretat i/o la declaració.	
I.3	Definir si serà necessària l'obtenció del consentiment dels ciutadans dels quals es tractaran les dades.	Només si es tractaran noves dades.
I.4	Definir els mecanismes mitjançant els quals s'executarà el deure d'informar als ciutadans.	Només si es tractaran noves dades.
I.5	Verificar que es té en compte en el procediment de gestió d'incidències les que puguin venir d'aquesta aplicació.	
I.6	Afegir clàusules al contracte de prestació de serveis per a que el proveïdor garanteixi que l'aplicació complirà els requeriments tècnics que requereix la normativa de protecció de dades.	Si el desenvolupament el fa un tercer.
I.7	Si el proveïdor ha d'accedir a les dades de caràcter personal, afegir al contracte de prestació de serveis les clàusules d'encarregat del tractament i informar al Responsable de Seguretat del nou encarregat. Si no ha d'accedir a les dades, afegir al contracte de prestació de serveis les clàusules de prohibició d'accés i la obligatorietat de guardar secret.	Si el desenvolupament el fa un tercer.

ID	Control	Comentaris
I.8	Formar als usuaris de l'aplicació en el tractament de dades de caràcter personal. Es pot complementar amb altres mecanismes com ara que l'aplicació mostri un text el primer cop que un usuari s'hi connecti i que s'obligui a la seva lectura i acceptació.	

4.1.2. Requeriments previs: disseny de l'aplicació

Respecte a l'aplicació, caldrà que es verifiqui que es contempla l'acompliment dels controls enumerats a continuació:

ID	Control	Comentaris
II.1	Verificar que les dades que hi ha a l'aplicació són les que s'han declarat	
II.2	Verificar que les dades que hi ha a l'aplicació no són excessives per a la finalitat declarada.	
II.3	Comprovar que existirà un mecanisme per bloquejar i cancel·lar dades.	
II.4	Si hi ha tractaments previstos als que el ciutadà es pot oposar, l'aplicació ha de permetre marcar-ho.	
II.5	Si hi ha cessions previstes a les que el ciutadà es pot oposar, l'aplicació ha de permetre marcar-ho.	
II.6	Si es permetrà recollir les dades provinents d'altres persones diferents de l'interessat, l'aplicació ha de permetre marcar-ho i mantenir les dades bloquejades fins que s'hagi informat a l'afectat i, si s'escau, obtingut el seu consentiment.	Només si es tractaran noves dades.
II.7	Si en l'aplicació hi ha formularis que emplena directament el ciutadà, caldrà que s'hi inclogui els texts legals del deure d'informació, i consentiment, si s'escau.	

4.2. Controls de seguretat

A continuació s'enumera el conjunt de controls i mesures tècniques de seguretat que cal implementar en les aplicacions que tractin dades de caràcter personal de nivell alt.

4.2.1. Fitxers temporals

ID	Control	Comentaris
III.1	Qualsevol fitxer temporal que l'aplicació hagi de generar durant el procés de les dades ha d'estar sotmès al mateix nivell de seguretat que les dades originals. Es recomana que els fitxers temporals amb dades personals que s'hagin de generar en zones o equips diferents de la base de dades on resideixin les dades originals, com per exemple en un servidor d'aplicacions, es creïn en zones protegides i d'accés restringit només per a aquests processos.	
III.2	Tot fitxer temporal que es generi s'ha d'eliminar després del seu procés garantint que es fa de manera que no es pugui recuperar la informació que contenia posteriorment. Cal implementar mecanismes per garantir que no quedin fitxers residuals amb dades de caràcter personal pels casos de fallides de processos o del sistema.	
III.3	Quan s'hagin de fer proves amb dades reals durant les fases de desenvolupament o integració es faran dissociant les dades prèviament, a menys que es pugui garantir el mateix nivell de seguretat a les dades durant tot el procés.	

4.2.2. Control d'accés

ID	Control	Comentaris
IV.1	L'accés a l'aplicació i a les dades que hi conté ha d'estar restringit només al personal autoritzat. Per tant, el sistema de gestió d'usuaris ha de permetre dotar a cada usuari d'una sèrie de permisos (perfil) que s'adeqüi als criteris necessaris definits. L'aplicació ha de permetre donar accessos diferenciats a diferents usuaris i diferents tipus de dades, i que aquests accessos puguin ser de només lectura, modificació, eliminació, etc.	

ID	Control	Comentaris
IV.2	S'ha de permetre que la creació dels perfils així com l'assignació d'aquests als usuaris només la puguin fer usuaris autoritzats a tal efecte.	
IV.3	S'ha de permetre la creació de llistats d'usuaris amb el perfil associat a cadascun. Aquesta funcionalitat també ha d'estar restringida a determinats usuaris.	
IV.4	Per tal de protegir les dades d'accessos diferents als que proporcioni la pròpia aplicació, cal limitar l'accés directe a les bases de dades.	

4.2.3. Identificació i autenticació

ID	Control	Comentaris
V.1	Cal garantir la identificació de forma inequívoca i personalitzada dels usuaris de l'aplicació, ja sigui pel codi d'usuari que hi accedeix o per qualsevol altre mecanisme d'identificació emprat. No es poden utilitzar usuaris genèrics o compartits que no permetin identificar la persona que accedeix a les dades.	
V.2	Cal garantir que l'usuari identificat és realment el que està usant l'identificador mitjançant mecanismes d'autenticació.	
V.3	Si les contrasenyes són pròpies de l'aplicació, cal emmagatzemar-les xifrades de manera que ningú, ni els administradors de l'aplicació, les puguin conèixer.	Només si l'autenticació es fa mitjançant contrasenyes.
V.4	Es recomana forçar el canvi de contrasenya després de la primera connexió d'un usuari nou.	Només si l'autenticació es fa mitjançant contrasenyes.
V.5	L'aplicació ha de comptar amb mecanismes que permetin la caducitat periòdica de la contrasenya. A més, la periodicitat s'ha de poder configurar per adaptar-la a la política definida. La caducitat mínima ha de ser d'un any, tot i que es recomana una periodicitat màxima de tres mesos.	
V.6	L'aplicació ha de limitar el nombre d'intents d'accés erronis de forma reiterada. En cas que es superi el límit, que s'ha de poder configurar, l'identificador d'usuari utilitzat ha de quedar bloquejat.	

4.2.4. Còpies de seguretat i restauració

ID	Control	Comentaris
VI.1	L'aplicació ha de permetre que es generin còpies de seguretat de les dades de caràcter personal.	
VI.2	L'aplicació ha de permetre que es generin còpies de seguretat en suports externs per tal que es puguin transportar a una ubicació alternativa a on es trobin els sistemes.	

4.2.5. Registre d'accessos

ID	Control	Comentaris
VII.1	L'aplicació ha de generar un registre de cada accés a les dades de caràcter personal. Aquest registre ha de contenir: ▪ Identificació de l'usuari ▪ Data i hora ▪ Fitxer accedit ▪ Tipus d'accés ▪ Accés autoritzat o denegat ▪ La informació que permeti identificar les dades accedides, sempre i quan l'accés hagi estat autoritzat	
VII.2	El registre ha de permetre fer consultes al seu contingut	
VII.3	El registre no pot ser manipulat ni alterat per cap usuari.	
VII.4	S'ha de garantir que el registre podrà ser accedit només a usuaris autoritzats a tal efecte, i que aquests disposaran de mecanismes per a revisar-los periòdicament i fer-ne informes.	

4.2.6. Telecomunicacions

ID	Control	Comentaris
VIII.1	S'ha de preveure que qualsevol transmissió de les dades personals es pugui fer xifrada si aquesta transmissió es preveu que es farà a través de xarxes públiques (per exemple, Internet) o a través de qualsevol tipus de xarxa sense fils (per exemple, WiFi). Sota aquestes circumstàncies l'accés dels usuaris s'ha de fer mitjançant mecanismes que xifrin les dades personals, ja sigui mitjançant protocols de xifrat estàndard (per exemple, https si l'accés és via web) o mitjançant solucions propietàries.	
VIII.2	Es considera també transmissió de dades els processos en els quals no intervinguin els usuaris, com la transmissió entre capes de la pròpia aplicació si aquestes es troben en sistemes diferenciats, o com la transmissió de les dades a sistemes de backup.	

4.3. Bones pràctiques

A continuació s'enumera el conjunt de controls i mesures tècniques de seguretat que, tot i no ser d'obligat compliment segons la normativa vigent de protecció de dades, es consideren bones pràctiques i per tant caldria implementar en les aplicacions que tractin dades de caràcter personal de nivell alt.

ID	Control	Comentaris
IX.1	Xifrar la transmissió de les contrasenyes en la fase d'autenticació i, en general, qualsevol transmissió d'informació.	
IX.2	Forçar l'ús de contrasenyes amb longituds mínimes de 8 caràcters.	
IX.3	Forçar l'ús de contrasenyes robustes amb números, caràcters no alfanumèrics i majúscules.	
IX.4	Utilitzar certificats digitals o sistemes biomètrics per a l'autenticació d'usuaris.	
IX.5	Utilitzar mecanismes de single-sign-on o delegar l'autenticació en sistemes centralitzats de gestió d'usuaris.	
IX.6	Implementar mecanismes de validació en la entrada de dades.	
IX.7	No emmagatzemar informació sensible en cookies ni en el codi font de les pagines web.	
IX.8	Forçar l'expiració de sessions després d'un període d'inactivitat d'un usuari.	
IX.9	Limitar la extracció de dades, generació d'informes, per part dels usuaris.	
IX.10	Realitzar auditories de seguretat de l'aplicació de forma periòdica.	
IX.11	Separar les dades de nivell alt de la resta, de manera que s'implementin majors controls de seguretat a les primeres. Addicionalment, no cal implementar el mecanisme de registre d'accessos per les dades que no són de nivell alt si aquestes es troben separades.	
IX.12	Implantar un procediment d'eliminació o bloqueig d'accessos per les baixes d'usuaris.	
IX.13	Implementar mecanismes per bloquejar de forma automàtica els usuaris després d'un determinat temps sense connectar-se a l'aplicació.	

ANNEX I. Decàleg de bones pràctiques en protecció de dades

1. Propietat de les dades

Les dades personals, com qualsevol dada identificativa (nom, adreça, DNI, telèfon, ...), de salut i situació social, fotografies, imatges, gravacions de veu, etc., pertanyen a les persones a les que es refereixen i només elles poden decidir sobre les mateixes. Per tant, ni tu ni cap organisme en sou propietaris.

2. Deure d'informació i consentiment

Cal verificar que s'informa de l'existència d'un fitxer, la seva finalitat, etc. a les persones quan es recullen les dades. Aquesta tasca la pots realitzar mitjançant uns formularis i impresos específics. A més, en determinades ocasions també caldrà que sol·licitis el consentiment explícit i per escrit de l'interessat.

Si les dades les proporciona una persona diferent a l'interessat (per exemple, una sol·licitud que lliura un familiar) cal iniciar el procediment establert per a que s'informi directament a l'afectat.

3. Qualitat de les dades

Les dades personals recollides han de ser adequades, pertinents i no excessives en relació amb la finalitat per a la qual es recullen. Així mateix, no es poden utilitzar per a una altra finalitat diferent.

4. Deure de secret

Has de mantenir, de forma indefinida i fins i tot si finalitzes la teva relació laboral actual, absoluta reserva i secret professional sobre qualsevol informació personal a la que tinguis accés en l'exercici de les teves funcions.

Estàs obligat a fer-ho per la normativa de protecció de dades i per la ètica professional. Tingues present que el seu incompliment por ser perseguit penalment.

5. Comunicar les incidències.

Cal que comuniquis el més aviat possible als responsables dels fitxers qualsevol anomalia que afecti a la seguretat de les dades personals que tractes. Això inclou qualsevol alteració o pèrdua de dades així com qualsevol incidència amb els teus identificadors o contrasenyes.

6. Mesures de seguretat

És la teva obligació complir la normativa de seguretat en matèria de dades personals. Si no te l'han entregada, cal que la reclamis. No oblidis:

- Utilitza les teves contrasenyes i no les comparteixis.
- Guarda els documents amb dades personals en armaris i calaixos tancats quan no hi siguis davant.
- Cal que mantinguis les dades personals fora de la vista de persones no autoritzades, ja sigui documentació en paper o en la pantalla de la teva estació de treball a través d'una aplicació.
- Bloqueja la sessió sempre que t'allunyis de l'estació de treball.
- Has de tenir cura de no deixar documents amb dades personals en fotocopiadores, impressores, faxos o fins i tot a sobre d'una taula.
- Compleix les mesures de seguretat si t'enduus dades en portàtils memòries USB, CD's o DVD's i documentació impresa.

7. Destrucció de dades

Has de garantir que les dades no seran accessibles un cop les hagis d'eliminar. Per exemple, la documentació en paper s'ha d'eliminar mitjançant una destructora de papers o un procediment similar.

8. Exercici dels drets

Has de facilitar als ciutadans l'exercici dels seus drets d'accés, rectificació, cancel□lació i oposició. Has de proporcionar-los els impresos adequats.

9. Cessió o comunicació de dades

No és permès enviar dades a tercers mitjançant cap tipus de suport material o qualsevol altre mitjà de comunicació, incloent-hi la simple visualització, el correu electrònic o el fax.

10. Més preguntes?

Qualsevol dubte que tinguis en relació al tractament de dades personals dirigeix-lo al teu responsable. La privacitat de les dades és una responsabilitat de tots.

ANNEX II. Clàusules estàndard de protecció de dades

II.1. Dret d'informació i recollida de consentiment

Les següents clàusules s'han d'utilitzar per tal de garantir el dret dels ciutadans a ser informats de la recollida i tractament de les seves dades, i per a recollir-ne el seu consentiment. Es distingeixen tres casos:

- Les dades es recullen del propi interessat,
- Les dades es recullen de fonts accessibles al públic, o bé
- Les dades es recullen d'una persona diferent al propi interessat.

II.1.1. Dades lliurades pel propi interessat i recollides en formularis

La següent clàusula ha de ser afegida en tots els formularis de recollida de dades que s'utilitzin per a qualsevol servei d'Acció Social, per tal d'informar al ciutadà de la finalitat del tractament de les seves dades i recollir-ne el seu consentiment:

> *De conformitat amb la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, l'informem que les seves dades personals s'incorporaran en un fitxer del qual és titular el* ***Sector de Serveis Personals*** *de l'Ajuntament de Barcelona, amb les finalitats de <desenvolupar els Programes i Competències que la Llei d'Acció Social de la Generalitat de Catalunya assigni a l'Ajuntament de Barcelona / proporcionar ajuts socials, viatges per gent gran i altres activitats emmarcades en l'àmbit de la prestació de serveis socials als ciutadans i residents de la ciutat / proporcionar ajuts a la regularització legal i laboral d'immigrants>*[1]*. Les seves dades no seran cedides a cap altra entitat, excepte en els supòsits contemplats per la llei. Consentiu expressament en el tractament de les seves dades per la finalitat indicada. Finalment, l'informem que podreu exercitar en qualsevol moment els drets d'accés, rectificació, cancel□lació i oposició en els termes establerts en la legislació vigent sobre protecció de dades, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte* ***Exercici de Dret LOPD****.*

Si es sol□licita també el consentiment per a una finalitat que no guardi relació directa amb la prestació dels serveis d'Acció Social (per exemple, utilitzar una fotografia d'un infant per a una campanya publicitària posterior), s'haurà de permetre al ciutadà expressar la negativa a consentir aquest tractament o cessió. En particular es pot utilitzar un mecanisme on el ciutadà pugui marcar una casella clarament visible que no estigui prèviament marcada.

[1] Eliminar les finalitats que no siguin escaients.

Si es recullen dades de creences, ideologia, religió o afiliació sindical, caldrà sempre indicar el dret del ciutadà a no proporcionar aquestes dades (optatives), ja que segons l'article 16 de la Constitució ningú pot ser obligat a declarar sobre aquestes dades.

Si el formulari on es recullen les dades no inclou l'acceptació del ciutadà amb el seu nom complert, data i signatura, caldrà recollir-la en un full annex al formulari; en aquest cas, la clàusula anterior es trobarà en aquest annex.

II.1.2. Dades recollides de fonts accessibles al públic

Quan les dades són recollides de fonts accessibles al públic, i és la primera vegada que es recullen per a una mateixa finalitat, cal informar a l'usuari en un termini màxim de tres mesos.

Aquesta acció es pot dur a terme enviant un escrit a l'interessat a l'adreça que consti del mateix, o bé en el padró municipal d'habitants. En l'escrit caldrà afegir la següent clàusula per tal d'informar al ciutadà de l'origen de les dades, la finalitat del tractament i recollir-ne el seu consentiment:

> *De conformitat amb la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, l'informem que les seves dades personals, recollides de la font accessible al públic <nom de la font>[2], s'incorporaran en un fitxer del qual és titular el* ***Sector de Serveis Personals*** *de l'Ajuntament de Barcelona, amb les finalitats de <desenvolupar els Programes i Competències que la Llei d'Acció Social de la Generalitat de Catalunya assigni a l'Ajuntament de Barcelona / proporcionar ajuts socials, viatges per gent gran i altres activitats emmarcades en l'àmbit de la prestació de serveis socials als ciutadans i residents de la ciutat / proporcionar ajuts a la regularització legal i laboral d'immigrants>[3]. Les seves dades no seran cedides a cap altra entitat, excepte en els supòsits contemplats per la llei.*
>
> *S'entendrà que consentiu expressament en el tractament de les seves dades per la finalitat indicada si en el termini de trenta dies a comptar des de la recepció d'aquest no ha expressat la seva negativa explícita al tractament, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte* ***Exercici de Dret LOPD*** *.*

[2] Especificar la font accessible al públic, per exemple, cens promocional, llistats de persones pertanyents a un col·lectiu professional, guies de serveis de comunicacions electròniques, Diaris oficials, etc.
[3] Eliminar les finalitats que no siguin escaients.

Finalment, l'informem que podreu exercitar en qualsevol moment els drets d'accés, rectificació, cancel·lació i oposició en els termes establerts en la legislació vigent sobre protecció de dades, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte ***Exercici de Dret LOPD****.*

Es recomana adjuntar un sobre pre-franquejat per tal de facilitat al ciutadà la negativa al tractament de les seves dades.

En el casos en què calgui el consentiment explícit de la persona, caldrà sol·licitar l'acceptació firmada per part de l'usuari. Es recomana adjuntar un sobre pre-franquejat per tal de facilitar al ciutadà la resposta. Mentre no s'obtingui el consentiment les dades hauran d'estar bloquejades i no es podran tractar. Els casos en què cal el consentiment explícit són:

- Si es sol·licita també el consentiment per a una finalitat que no guardi relació directa amb la prestació dels serveis d'Acció Social (per exemple, utilitzar una fotografia d'un infant per a una campanya publicitària posterior).
- Si es recullen dades de creences, ideologia, religió o afiliació sindical, ja que segons l'article 16 de la Constitució ningú pot ser obligat a declarar sobre aquestes dades.

El text que cal utilitzar és la següent:

De conformitat amb la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, l'informem que les seves dades personals, recollides de la font accessible al públic <nom de la font>[4], s'incorporaran en un fitxer del qual és titular el ***Sector de Serveis Personals*** *de l'Ajuntament de Barcelona, amb les finalitats de <desenvolupar els Programes i Competències que la Llei d'Acció Social de la Generalitat de Catalunya assigni a l'Ajuntament de Barcelona / proporcionar ajuts socials, viatges per gent gran i altres activitats emmarcades en l'àmbit de la prestació de serveis socials als ciutadans i residents de la ciutat / proporcionar ajuts a la regularització legal i laboral d'immigrants>[5]. Les seves dades no seran cedides a cap altra entitat, excepte en els supòsits contemplats per la llei.*

[4] Especificar la font accessible al públic, per exemple, cens promocional, llistats de persones pertanyents a un col·lectiu professional, guies de serveis de comunicacions electròniques, Diaris oficials, etc.
[5] Eliminar les finalitats que no siguin escaients.

Consentiu expressament en el tractament de les seves dades per la finalitat indicada. Finalment, l'informem que podreu exercitar en qualsevol moment els drets d'accés, rectificació, cancel·lació i oposició en els termes establerts en la legislació vigent sobre protecció de dades, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte ***Exercici de Dret LOPD****.*

Nom complert, data i signatura:

II.1.3. Dades lliurades per una persona diferent del propi interessat

Quan les dades són lliurades per persones diferents del propi interessat (per exemple, quan un familiar lliura una sol·licitud), i és la primera vegada que es recullen per a una mateixa finalitat, cal informar a l'usuari en un termini màxim de tres mesos.

Aquesta acció es pot dur a terme enviant un escrit a l'interessat a l'adreça que consti del mateix, o bé en el padró municipal d'habitants. En l'escrit caldrà afegir la següent clàusula per tal d'informar al ciutadà de l'origen de les dades, la finalitat del tractament i recollir-ne el seu consentiment:

De conformitat amb la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, l'informem que les seves dades personals s'incorporaran en un fitxer del qual és titular el ***Sector de Serveis Personals*** *de l'Ajuntament de Barcelona, amb les finalitats de <desenvolupar els Programes i Competències que la Llei d'Acció Social de la Generalitat de Catalunya assigni a l'Ajuntament de Barcelona / proporcionar ajuts socials, viatges per gent gran i altres activitats emmarcades en l'àmbit de la prestació de serveis socials als ciutadans i residents de la ciutat / proporcionar ajuts a la regularització legal i laboral d'immigrants>*[6]*. Les seves dades no seran cedides a cap altra entitat, excepte en els supòsits contemplats per la llei.*

S'entendrà que consentiu expressament en el tractament de les seves dades per la finalitat indicada si en el termini de trenta dies a comptar des de la recepció d'aquest no ha expressat la seva negativa explícita al tractament, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte ***Exercici de Dret LOPD*** *.*

Finalment, l'informem que podreu exercitar en qualsevol moment els drets d'accés, rectificació, cancel·lació i oposició en els termes establerts en la legislació vigent sobre protecció de dades, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte ***Exercici de Dret LOPD****.*

[6] Eliminar les finalitats que no siguin escaients.

Es recomana adjuntar un sobre pre-franquejat per tal de facilitat al ciutadà la negativa al tractament de les seves dades.

En el casos en què calgui el consentiment explícit de la persona, caldrà sol□licitar l'acceptació firmada per part de l'usuari. Es recomana adjuntar un sobre pre-franquejat per tal de facilitar al ciutadà la resposta. Mentre no s'obtingui el consentiment les dades hauran d'estar bloquejades i no es podran tractar. Els casos en què cal el consentiment explícit són:

- Si es sol□licita també el consentiment per a una finalitat que no guardi relació directa amb la prestació dels serveis d'Acció Social (per exemple, utilitzar una fotografia d'un infant per a una campanya publicitària posterior).
- Si es recullen dades de creences, ideologia, religió o afiliació sindical, ja que segons l'article 16 de la Constitució ningú pot ser obligat a declarar sobre aquestes dades.

El text que cal utilitzar és la següent:

De conformitat amb la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, l'informem que les seves dades personals s'incorporaran en un fitxer del qual és titular el ***Sector de Serveis Personals*** *de l'Ajuntament de Barcelona, amb les finalitats de <desenvolupar els Programes i Competències que la Llei d'Acció Social de la Generalitat de Catalunya assigni a l'Ajuntament de Barcelona / proporcionar ajuts socials, viatges per gent gran i altres activitats emmarcades en l'àmbit de la prestació de serveis socials als ciutadans i residents de la ciutat / proporcionar ajuts a la regularització legal i laboral d'immigrants>*[7]*. Les seves dades no seran cedides a cap altra entitat, excepte en els supòsits contemplats per la llei.*

Consentiu expressament en el tractament de les seves dades per la finalitat indicada. Finalment, l'informem que podreu exercitar en qualsevol moment els drets d'accés, rectificació, cancel□lació i oposició en els termes establerts en la legislació vigent sobre protecció de dades, adreçant-vos per escrit al Registre General de l'Ajuntament: Pl. San Miquel 5-6, 08002 Barcelona, indicant clarament en l'assumpte ***Exercici de Dret LOPD****.*

Nom complert, data i signatura:

[7] Eliminar les finalitats que no siguin escaients.

II.2. Contractes de prestació de serveis amb accés a les dades personals

La següent clàusula ha de ser afegida en tots els plecs de condicions o contractes per als quals es demana un encàrrec de tractament a tercers, això és, l'adjudicatari tindrà accés a les dades de caràcter personal en l'exercici de les tasques que li són encomanades:

1. *El contractista s'obliga a tractar les dades de caràcter personal a les quals tingui accés en ocasió del compliment del contracte d'acord amb les instruccions dictades per l'Ajuntament de Barcelona, sense que en cap cas les pugui aplicar ni utilitzar amb una finalitat diferent a aquel1 compliment, ni comunicar-les, ni tan sols per a la seva conservació, a d'altres persones.*

2. *El contractista resta obligat al secret professional pel que fa a les dades de caràcter personal a les quals tingui accés en ocasió del compliment del contracte, obligació que subsisteix fins i tot després, una vegada resolt el contracte.*

   Així mateix, el contractista ha de guardar reserva respecte de les dades o antecedents que no siguin públics o notoris dels quals hagi tingut coneixement en ocasió del contracte. En aquest sentit, la documentació i informació a la qual tingui accés el contractista té caràcter confidencial, i no podrà ser objecte de reproducció total o parcial per cap mitjà o suport. Per tant, no se'n podrà fer cap tractament ni edició, informàtica o no, ni transmissió a terceres persones fora de l'estricte àmbit d'execució directa del contracte, ni tan sols entre la resta del personal que tingui o pugui tenir l'entitat que presta el servei objecte d'aquest.

   Si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, o si es fa de forma remota exclusivament a suports o sistemes d'informació de l'Ajuntament, el contractista té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa.

   Només podran accedir a les esmentades dades de caràcter personal, informacions i documentació les persones estrictament imprescindibles per al desenvolupament de les tasques inherents al propi contracte. Totes elles seran advertides pel contractista del caràcter d'informació confidencial i reservada i del deure de secret als quals estan sotmeses, i aquell serà responsable del compliment d'aquestes obligacions per part del seu personal.

3. *El contractista manifesta que té implantades les mesures de caràcter tècnic i organitzatiu necessàries per garantir la seguretat de les dades de caràcter personal a les quals tindrà accés en ocasió de l'execució del contracte, tot evitant-ne la seva alteració, pèrdua, tractament o accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a que estan exposades, i en estricte compliment de la normativa vigent en matèria de protecció de dades de caràcter personal.*

   D'acord amb allò que estableix el Reial Decret 1720/2007, de 21 de desembre, per el qual s'aprova el Reglament de Desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (LOPD), les mesures de seguretat implantades pel contractista són les corresponents al nivel1 <ALT/MIG/BAIX>[8], i són d'aplicació als fitxers, centres de tractament, locals, equips, sistemes, programes i persones que intervinguin en el tractament de les dades en els termes que estableix aquell reglament.

   El contractista queda obligat a realitzar un document de seguretat en els termes que estableix el Reial Decret 1720/2007 incorporant-hi les mesures de seguretat implantades.

   En tot cas, el contractista haurà de posar en coneixement de l'Ajuntament, immediatament després de ser detectada, qualsevol sospita o constatació d'eventuals errors o incidències que poguessin produir-se en el sistema de seguretat de la informació.

4. *L'Ajuntament de Barcelona podrà designar en qualsevol moment durant la vigència del contracte a personal intern o extern per a verificar que el contractista té implantades les mesures necessàries per garantir la seguretat de les dades de caràcter personal.*

5. *Durant la vigència del contracte. el contractista haurà de conservar qualsevol dada objecte de tractament, llevat que rebi indicacions en sentit contrari de l'Ajuntament de Barcelona.*

[8] Especificar el nivell de les dades a les quals tindrà accés el contractista. Donades les obligacions contractuals, no és escaient exigir mesures superiors a les necessàries.

6. *Una vegada executat el contracte, el contractista haurà de destruir ¡/o retornar a l'Ajuntament de Barcelona, d'acord amb allò que s'estableixi legalment o les indicacions que li transmeti aquest, les dades de caràcter personal que hagin estat objecte de tractament per part d'aquell durant la vigència del mateix, juntament amb els suports o documents en que consti alguna dada de caràcter personal. El retorn de les dades a l'Ajuntament es durà a terme en el format i els suports utilitzats pel contractista per al seu emmagatzematge.*

   En el cas que el contractista hagi de conservar necessàriament part de les dades en tant que es pugui derivar responsabilitats amb l'Ajuntament de Barcelona, haurà de bloquejar degudament les dades conservades per impedir-ne l'accés i el tractament.

7. *En el cas que destini les dades a les quals tingui accés a una finalitat diferent a l'establerta, o les comuniqui o les utilitzi incomplint les estipulacions del contracte o les instruccions de l'Ajuntament, el contractista serà considerat responsable del tractament i respondrà personalment de les infraccions que hagi comès i de les possibles reclamacions que es puguin produir al respecte.*

   L'Ajuntament repercutirà en el contractista els costos corresponents a les sancions i/o indemnitzacions a les que hagi de fer front que s'haguessin originat directa o indirectament pel deficient ¡/o negligent tractament de dades de caràcter personal realitzat pel contractista. En tot cas, el contractista s'obliga a mantenir indemne l'Ajuntament de totes les despeses o altres conseqüències negatives que se li puguin originar a causa dels esmentats tractaments, sancions i/o indemnitzacions.

II.3. Contractes de prestació de serveis amb subcontractació

Quan l'adjudicatari pugui subcontractar part del servei, caldrà afegir a la clàusula de prestació de serveis de l'apartat anterior la que s'adjunta a continuació.

En la mesura del possible, aquesta clàusula s'haurà d'adaptar a les diverses tipologies de plecs i de contractes administratius concrets que es poden celebrar, doncs com més ajustada estigui la seva redacció a l'objecte i naturalesa d'aquests, menys problemes interpretatius i de qualsevol altre ordre plantejarà la seva aplicació pràctica:

En el supòsit que el contractista hagués de subcontractar a un tercer l'execució parcial del contracte, i que aquesta execució comporti el tractament de dades de caràcter personal per part d'aquell, el contractista actuarà en nom i per compte de 1'Ajuntament.de Barcelona, el qual haurà d'autoritzar expressament i per escrit l'esmentada subcontractació.

Els licitadors, en les seves ofertes, hauran de preveure expressament quins serveis seran objecte de subcontractació i quines seran les empreses subcontractistes que els executaran. Prèvia autorització expressa de l'Ajuntament de Barcelona, aquestes previsions s'adjuntaran com a annex al contracte administratiu que es formalitzi, i qualsevol modificació de les mateixes requerirà l'autorització prèvia i per escrit de l'Ajuntament.

En tot cas, el tractament de dades realitzat per part del subcontractista haurà de complir amb la normativa vigent en matèria de protecció de dades de caràcter personal, i s'ajustarà així mateix a les obligacions assumides pel contractista i a les instruccions específiques que li doni l'Ajuntament de Barcelona al respecte

II.4. Contractes de prestació de serveis sense accés a les dades personals

La següent clàusula ha de ser afegida en tots els plecs de condicions o contractes per als quals es preveu que l'adjudicatari no tindrà accés a les dades de caràcter personal en l'exercici de les tasques que li són encomanades:

El contractista s'obliga a guardar reserva respecte a les dades o antecedents que no siguin públics o notoris i que estiguin relacionats amb l'objecte del contracte, dels quals hagi tingut coneixement amb ocasió del contracte.

Es prohibeix expressament l'accés a les dades de caràcter personal de l'Ajuntament de Barcelona per part del contractista. Aquest resta obligat al secret professional pel que fa a les dades de caràcter personal a les quals pugui tenir accés en ocasió del compliment del contracte, obligació que subsisteix fins i tot després, una vegada resolt el contracte

ANNEX III. Procediment de declaració

III.1. Procediment a seguir

Per tal de crear/modificar/suprimir un fitxer amb dades de caràcter personal cal:

Comunicar aquesta intenció a Informació de Base i Cartografia (IBC), usant com a model els fulls que hi ha a continuació i d'acord amb les instruccions i aclariments següents:

- IBC prepara informe favorable.
- El Sector corresponent demana informe jurídic.
- El Sector fa l'expedient necessari per la publicació en el BOP del Decret d'Aprovació Provisional (20 dies hàbils).
- El Sector publica al BOP el Decret d'Aprovació definitiva (incloent l'annex descriptiu d'aquesta plantilla) i comunica el núm. de BOP a IBC (temps mínim del procés: 2,5 mesos).

III.2. Aclariments i exemples

Instruccions prèvies

Les indicacions en color negre impliquen deixar-ho tal com està, el color blau vol dir substituir i el color vermell significa escollir una opció.

Aclariments a l'informe

Cal que hi constin la **necessitat explícita** de la creació o de la modificació del fitxer, justificada directament en l'activitat o servei públic municipal al qual respon el tractament, les **dades personals que han de ser objecte** del mateix, **l'interès públic** que es persegueix en cada cas i altres aspectes que considereu que poden ajudar a justificar la legitimitat del tractament de dades.

Penseu que, en cas hipotètic de conflicte, serà aquestes justificacions que constin al/s expedient/s les que ens hauran de servir per defensar el compliment de la LOPD, especialment pel que fa al principi fonamental de qualitat de les dades. Recordeu que aquestes consideracions permetrien la resposta a les al□legacions, si fos el cas.

Exemple:

> *Donat que la llei.....ens atorga les competències de ....., per tal de poder donar al ciutadà el servei ... i facilitar la tramitació administrativa cal crear i registrar a l'Agència de Protecció de Dades el fitxer següent.*

Aclariments a l'Annex

Nom del fitxer: Nom_del_Fitxer. Exemple: Padró Municipal d'Habitants, Projecte Jove, Impost de Vehicles de Tracció Mecànica.

Òrgans de l'Administració responsables del fitxer: Evitarem els Directors, en la mesura del possible. Exemples: Gerent de Seguretat i Mobilitat Ciutadana, Gerent de Serveis Generals, Gerent de Serveis Personals, Director de Recursos Humans.

Procediment pel qual es podran exercitar els drets d'accés, rectificació, cancel□lació i oposició: Descriure el procediment a emprar, tenint en compte que caldrà respondre en uns 10 dies. Exemple: carta adreçada a la Direcció d'Atenció al Ciutadà de l'Ajuntament de Barcelona, av. Diagonal, 240 08027 Barcelona, indicant clarament en el títol: **Tutela de drets LOPD**.

Nom del sistema i tipus de tractament: Per exemple:

> *El sistema SAT serà tractat de manera manual.*
>
> *El sistema Bicicletes serà tractat de forma automatitzada amb l'equip que accedeix mitjançant xarxa corporativa i intranet a les dades locals i dels servidors centrals.*

Encarregats de Tractament: Descripció de persones o empreses no municipals que maneguen les dades per compte del Responsable. Exemples: L'adjudicatari específic del plec de desbordament de servei (actualment ATENTO amb el Nif ...). Si fossin els concessionaris del Servei de Menjadors Socials o els Adjudicataris del plec d'impressió de... Si no hi ha cap en el moment de la declaració poden deixar-se en blanc en la declaració i explicitar-los en el document de seguretat (indicant en la declaració la clàusula d'encarregat de tractament a emprar en tots els contractes a signar en el futur).

Estructura bàsica del fitxer i nivell de seguretat requerit: Cal només deixar el tipus i descripció de dades que emprarà el fitxer. (si ara no s'utilitzen, però és previsible fer-ho, cal posar-les per evitar un nou expedient de modificació del fitxer).

El tipus "infraccions" i "dades especialment protegides" tenen requeriments de seguretat específics (mig o alt respectivament). Les dades d'impostos i taxes, si especifiquen quan i com no s'han liquidat, es consideren infraccions administratives. Una acumulació de dades de nivell baix requeriria també requeriments de seguretat de nivell mig.

Finalitat del fitxer i usos previstos: Descripció prou genèrica de la finalitat, que cobreixi les necessitats de tractament de dades actuals i futures, però prou concreta per satisfer la normativa. Per exemple, manteniment de les dades de les persones que han iniciat un tràmit. Aquella/es que hem comunicat als afectats o que, si no els comuniquem explícitament, s'infereixen del tipus de dades i el context on es demanen. Haurà d'estar explícitament declarada a l'APD, ergo, modificar-la implicarà una modificació del fitxer. Cal tipificar les finalitats per categories relatives a recursos humans, a hisenda i gestió econòmico-financera, a justícia, a seguretat pública i defensa, a treball i benestar social, a sanitat, a educació i cultura, a estadística, d'altres finalitats (tot eliminant les no desitjades de les llistades).

Persones o col□lectius sobre les que es pretengui obtenir dades de caràcter personal: Descripció de les persones o col□lectius sobre els quals s'obtenen les dades personals o que resultin obligats a subministrar-les, descripció de la categoria de persones objecte de tractament. Persona física o jurídica que iniciï un tràmit. Per exemple: ciutadans que sol□liciten informació sobre matriculació en escoles públiques.

Procediment de recollida de les dades de caràcter personal: Especificar les operacions i els procediments tècnics de caràcter automatitzat o no, que permetin recollir les dades. Especifiqueu els procediments actuals i cobriu els futurs raonablement coneguts (per minimitzar la necessitat de modificacions que requereixin repetir l'aprovació). Per exemple: formularis web o paper o telemàtics emplenats per l'interessat. Gravació de dades en càmeres instal□lades al vestíbul de l'edifici.

Cessions de dades de caràcter personal: Cal fer una descripció exhaustiva de totes les cessions previstes i normativa o consentiment que les empara, o caracterització d'elles (cessions diferents o d'altre tipus requeriran un nou expedient de modificació de la declaració). Típicament estarà buit o contindrà:

> *Les dades no seran comunicades a terceres persones, excepte en cas d'ésser sol□licitades pel Síndic o Defensor del Poble o bé pel Ministeri Fiscal, Jutges o Tribunals en l'exercici de les funcions que tenen atribuïdes (cessió emparada per l'article 11 de la LOPD).*

Exemples:

Les dades no seran cedides a tercers.

Les dades es recullen per compte del Departament d'Habitatge de la Generalitat.

Les dades no seran comunicades a terceres persones, excepte en els supòsits legalment establerts o quan l'interessat hagi atorgat previ consentiment, o en altres administracions amb competències en Benestar Social d'acord amb la Llei .....

Transferències de dades previstes a països tercers: Cal fer una descripció exhaustiva de totes les transferències previstes i normativa o consentiment que les empara, especificant, si s'escau, l'existència d'informe de l'AEPD respecte a la idoneïtat de la transferència o raó que justifiqui el nivell de seguretat del país tercer.

Motivació del canvi (només si ja existia): Si no hi hagués canvi de declaració, eliminar la línia.

Responsable operatiu de les dades: Nom i telèfon de la persona del departament amb la qual l'IMI pot contactar per tal de verificar algun punt que calgui millorar, tant en l'actualitat com per resoldre dubtes, drets d'accés i accions operatives en el futur.

Ajuntament de Barcelona

Institut Municipal d'Informàtica
Informació de Base i Cartografia

Av. Diagonal 220, 5a
08018 Barcelona
Telèfon 291 81 00
Telefax 291 83 33

Petició de Creació/Modificació d'un nou Fitxer Municipal amb Dades de Caràcter Personal i posterior inscripció al Registre de l'Agencia de Protecció de Dades.

Donat que la llei.....ens atorga les competències de ....., per tal de simplificar la tramitació administrativa, per raons organitzatives del servei i com a resultat de la dinàmica municipal cal crear i inscriure al registre de l'Agència de Protecció de Dades el fitxer següent:

- Nom del fitxer.....

Per tant i per tal d'iniciar l'expedient d'aprovació/creació/modificació del fitxer, que tramitarà el nostre Sector, us demano informe tècnic respecte de la necessitat de crear aquest fitxer amb dades de caràcter personal d'acord amb el nom, finalitat, contingut, afectats, etc. descrites a l'annex.

Així mateix us demano que, un cop aprovat pel corresponent òrgan municipal i publicat al Butlletí Oficial, trameteu la declaració d'aquest fitxer al Registre de l'Agència de Protecció de Dades Catalana.

Atentament,

vist-i-plau

Director de .....

Gerent de .....

Ajuntament de Barcelona

Institut Municipal d'Informàtica
Informació de Base i Cartografia

Av. Diagonal 220, 5a
08018 Barcelona
Telèfon 291 81 00
Telefax 291 83 33

Annex 1. Fitxer *Nom_del_Fitxer*

Òrgans de l'Administració responsables del fitxer: Persona física o jurídica, de naturalesa pública o privada, u òrgan administratiu que decideixi sobre la finalitat, el contingut i l'ús del tractament.

Procediment pel qual es podran exercitar els drets d'accés, rectificació, cancel·lació i oposició: Carta adreçada a l'òrgan administratiu responsable del fitxer i lliurada al Registre Municipal, indicant clarament en el títol: **Tutela de drets LOPD.**

Nom del sistema i tipus de tractament: El sistema nom_del_sistema_d'informació serà tractat de forma automatitzada/manual amb equips que accedeixin mitjançant xarxa corporativa/de forma autònoma emprant intranet/Internet a servidors centrals/equip local.

Encarregats de Tractament: Persona física o jurídica, l'autoritat pública, el servei o qualsevol altre organisme que, sol o conjuntament amb els altres, tracti dades personals per compte del responsable del tractament.

Estructura bàsica del fitxer i nivell de seguretat requerit: El fitxer inclourà les dades de caràcter personal del tipus següent:

- **identificatives:** DNI/NIF, núm. Seg. Social/mútua, nom i cognoms adreça, e-mail, telèfon, signatura/empremta, imatge/veu, marques físiques, núm. reg. personal, signatura electrònica.
- **personals:** estat civil, dades familiars, data naixement, lloc naixement, edat, sexe, nacionalitat, llengua materna, llengua vehicular preferent, característiques físiques o antroponomètriques.
- **socials:** allotjament o habitatge, situació militar, propietats, possessions, aficions, estils de vida, clubs/associacions, llicències, permisos i autoritzacions.
- **professionals:** formació, titulació, historial estudiantil, experiència, pertany a col·legis/associacions professionals.
- **treball:** cos/escala, categoria/grau, lloc de treball, dades no econòmiques de la nòmina, historial laboral, altres.
- **comercial:** activitats i negocis, llicències comercials, subscripcions (revistes, web's,...), creacions artístiques, científiques o tècniques.
- **econòmico-financeres:** ingressos, rendes, inversions/patrimoni, crèdits/avals, dades bancàries, plans de pensió o jubilació, dades econòmiques de la nòmina, impostos/deduccions, assegurances, hipoteques, subsidis/beneficis, historial de crèdits, targes de crèdit.
- **transaccions:** bens i serveis subministrats, id. rebuts, transaccions financeres, compensacions/indemnitzacions.
- **infraccions:** penals, administratives.
- **especialment protegides:** ideologia, afiliació sindical, religió, creences, origen racial o ètnic, salut (malalties, discapacitats...), vida sexual, violència de gènere.

Finalitat del fitxer i usos previstos: Descripció detallada de la finalitat i els usos previstos. Especificar els tipus de finalitats a emprar. Aquestes finalitats es concreten en la tipologia:

- **Recursos humans:** gestió de personal, gestió de nòmina, formació, fons d'acció social, oposicions i concursos, riscos laborals, control horari, incompatibilitats i patrimoni alts càrrecs.
- **Hisenda i gestió econòmica financera:** recaptació tributària, gestió econòmica, facturació, gestió fiscal, deute i tresoreria, gestió cadastral, relacions comercials, regulació mercats financers, defensa competència.
- **Justícia:** procediments judicials, registres de fe pública, prestació social substitutòria, tramitació d'indults.
- **Seguretat pública i defensa:** protecció civil, seguretat vial, actuacions policials, actuacions administratives, institucions penitenciàries, servei militar, visats de residència.
- **Treball i Benestar Social:** promoció ocupació, relacions laborals, inspecció i protecció social, formació ocupacional, prestació atur, prestació garantia salarial, prestacions assistència social, pensions i subsidis i altres prestacions, acció immigrants, minusvalies, tercera edat, promoció social de la dona, joventut, protecció de menors, toxicomanies, accés a l'habitatge, altres serveis socials.
- **Sanitat:** gestió i control sanitari, historials clínics, investigació epidemiològica, targeta sanitària.

Institut Municipal d'Informàtica
Informació de Base i Cartografia

Av. Diagonal 220, 5a
08018 Barcelona
Telèfon 291 81 00
Telefax 291 83 33

- **Educació i Cultura:** educació infantil i primària, ensenyament secundari, ensenyament superior, estudis artístics i idiomes, educació especial, beques i ajuts a l'estudi, esports, foment d'activitats culturals, patrimoni històric i/o artístic
- **Estadística:** estadística pública, padró d'habitants, cens promocional, enquestes sociològiques i d'opinió
- **Altres:** procediments adm., registres de documents, altres registres adm., atenció al ciutadà, autoritzacions i permisos, control d'accés a edificis, publicacions, finalitats històriques i científiques, gestió de sancions, estadístiques internes, serveis de certificació, altres finalitats.

Persones o col·lectius sobre les que es pretengui obtenir dades de caràcter personal: Persona física o jurídica titular de les dades que siguin objecte del tractament de dades.

Procediment de recollida de les dades de caràcter personal: Recollides: del propi interessat o del seu representant; O bé mitjançant cessió consentida per l'interessat de dades dels serveis municipals/... (descriure'ls), o de Registres públics o d'Administracions públiques o d'Entitats privades o de Fons accessibles al públic (cens promocional, guies de serveis de telecomunicacions, llistes de grups professionals, diaris oficials, mitjans de comunicació). Mitjançant enquestes o entrevistes, formularis, transmissió electrònica, o altres (cas d'emprar altres, cal detallar-les) . Utilitzant: suport paper, magnètic o digital, via telemàtica, altres (cas d'emprar altres, cal detallar-les).

Cessions de dades de caràcter personal: Supòsits en els quals s'empara la cessió o comunicació de dades, que és qualsevol revelació de dades efectuada a una persona diferent de l'interessat.

Transferències internacionals de dades: Supòsits legals que habiliten la realització de la transferència internacional de dades.

Motivació del canvi: descripció de les raons tècnic jurídiques que fan necessari els canvis en la declaració del fitxer. (eliminar si es tracta de la creació d'un nou fitxer).

Responsable operatiu de les dades: Persona del departament amb qui podem contactar.